#3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2001 (27.12.2001)

PCT

(10) International Publication Number
WO 01/98934 A2

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number: PCT/US01/19617

(22) International Filing Date: 20 June 2001 (20.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/597,265 20 June 2000 (20.06.2000) US

(71) Applicant *(for all designated States except US)*: **INFONUTZ, LLC** [US/US]; Suite 301, 6320 Agusta Drive, Springfield, VA 22150 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MORTL, William, M.** [US/US]; 19 Woodenbridge Drive, Yorkville, IL 60560 (US).

(74) Agents: **GADIANO, Willem, F.** et al.; McDermott, Will & Emery, 600 13th Street, NW, Washington, DC 20005-3096 (US).

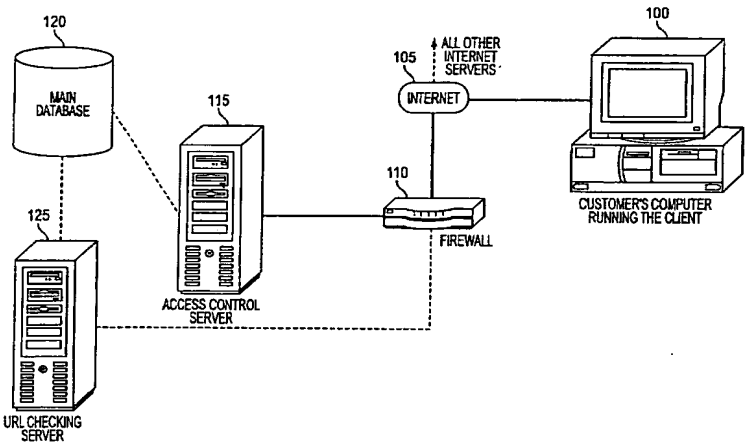
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR GRANTING ACCESS TO INTERNET CONTENT



(57) Abstract: An Internet content filtering software comprises two components. One component runs on an Internet server and the other component runs locally on a user's computer system. The two components cooperate with one another to filter Internet content, with each component performing separate tasks. The Internet server component stores user profiles, a list and/or a table of permitted and prohibited Uniform Resource Locators (URLs), and receives redirected URL requests. Redirected URL requests are utilized, in conjunction with a user's profile, to determine whether access is granted or denied to the content associated with the URL. The component running locally on a user's computer system acts as a client to the Internet server component, performing logon functions for a user, scanning Internet content associated with permitted URLs , and updating the Internet server component with a URL, indicating that the URL is prohibited if a predefined word or phrase is located in the Internet content associated with the URL. The Internet filtering software arrangement permits the same level of filtering to be applied to a user no matter where the user accesses the Internet from, as long as the computer system is running the second component, i.e., the client software.

WO 01/98934 A2

BNSDOCID: <WO___0198934A2_I_>

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BNSDOCID: <WO___0198934A2_I_>

METHOD AND APPARATUS FOR GRANTING ACCESS TO INTERNET CONTENT

FIELD OF THE INVENTION

The present invention generally relates to novel methods for providing filtering of Internet content.

BACKGROUND OF THE INVENTION

The Internet is a vast collection of information resources from around the world contained on millions of computers, each with their own individual properties and content. Computers connected to the Internet are often linked to a network which is in turn liked to other networks etc., enabling a computer connected to the Internet to access information stored on the millions of other computers linked to the networks that form the Internet. Because of the individualized nature of linking a computer, or a network of computers, to the Internet, there is no central regulation over the Internet, and therefore no regulation of the content available over the Internet. While this lack of regulation stimulates growth and addition of new materials on a daily basis, it also creates problems relating to access to inappropriate materials in various circumstances.

Many computers connected to the Internet contain documents written in the Hypertext Mark-up Language ("HTML") that are publicly viewable, and are easy to find and access. These HTML documents that are available for public use on the Internet are commonly referred to as "Web Pages". All of the computers that host web pages comprise what is known today as the World Wide Web ("WWW").

The WWW is comprised of an extremely large number of web pages that is growing at an exponential rate every day. A naming convention known as the Uniform Resource Locator ("URL") is used to designate every web page on the Internet. Web pages are typically assigned to the URL subclass known as the Hypertext Transport Protocol ("http") while other subclasses exist for file servers, information servers, and other machines present on the Internet. URLs are an important part of the Internet in that they are responsible for locating a web page and hence, for locating desired information.

World Wide Web users typically type in a URL, or use a search engine to locate URLs associated with web pages containing the type of information the WWW user is seeking. "Linking" is another method of providing URLs to an Internet user. When a user accesses any given web page via a URL, "links" to other URLs may be present on the web

page. This expanding directory structure is seemingly infinite, and leads a user seeking one web page, to potentially hundreds of web pages that were previously unknown and/or unsought by that user.

Using these technologies, large amounts of information covering a wide variety of topics are available on the WWW and are easily accessible by anyone who has Internet access. In many situations, however, it is desirable to limit the amount and type of information that certain individuals are permitted to retrieve. For example, in an academic setting it is undesirable for students to view pornographic or violent content while accessing the WWW via school resources. It is also not possible for parents to constantly monitor their children while using the WWW at home. Programs have been developed, purportedly to allow employers to keep track of what employees view while using the WWW at work. However, it is not practical to use such tracking to control access by a substantial number of employees in real-time. Many situations exist where inappropriate material, of a pornographic nature or otherwise, can be accessed using the WWW, and it is desirable to limit such access.

Solutions for filtering inappropriate content from the WWW are limited, especially in an academic setting. Schools either ignore inappropriate material available on the WWW, or attempt to filter it with software originally designed for home use on a single computer. Current filtering software is available in two basic forms, "site blocking" and "content filtering."

Site blocking software are essentially programs that intercept a requested URL after a computer user has typed or selected the requested URL into an Internet browser, and transmitted the URL request to the Internet. Site blocking software screen for inappropriate content by attempting to match the intercepted URL with a URL from a list or table of known Internet sites containing inappropriate content. If a match is found, then the site blocking software does not allow the URL request to be completed. For example, a user receives an "access denied" message instead of the web page associated with the requested URL. The main disadvantage associated with site blocking software is the rapid addition and modification of Internet sites. Such additions and modifications make the most up-to-date software obsolete within a few short weeks.

Site blocking software has two basic forms. One form of site blocking software actually comprises a list of approved sites that a user may view on the WWW. Such approved site software works by controlling where on the WWW a user can browse by limiting browsing to sites on the approved list. A major disadvantage of approved site

software is that it is very limiting regarding what information is available via the WWW, and is over-inclusive in what it blocks when applied to a large number of persons, e.g., in an academic setting. The second form of site blocking software basically comprises a list of sites that are prohibited, and prevents users from visiting those prohibited sites on the WWW. A major disadvantage to prohibited site software is the rapidity with which existing sites are modified and new sites are added to the WWW (some estimate that 150,000 site names are either modified or added per month). Unless the list of prohibited sites is updated frequently, it quickly becomes obsolete for purposes of denying access to inappropriate material available via the WWW. However, frequently updating the list of prohibited sites has several drawbacks. In order to add new site names to the list, many software vendors employ people to surf the WWW searching for web pages containing inappropriate material. Paying employees to surf the WWW is expensive, and is also an inefficient method for identifying new sites with inappropriate content, as there is no manner to determine whether a new site has already been identified by another employee. Another drawback is the need to either "push" a new prohibited site list to everyone utilizing the software vendor's program over the Internet, or the need to download a recent copy of the prohibited site list from the Internet. Both methods are time consuming and require human intervention in order to effectuate them.

Another approach to the problem involves content scanning software, which attempts to "read" a web page to identify prohibited words or phrases, and then stops the download of the page once a prohibited word or phrase is identified. Content filtering software allow the computer user's URL request to retrieve the web page associated with the requested URL. However, the content filtering software performs a read operation, i.e., scans the incoming information line-by-line, and constantly compares the read information with a list of words and phrases. If a match is found between incoming information and the list of words and phrases, then the content filtering software terminates the download of the web page. Some content filtering programs also attempt to scan images as they are downloaded, however, image scanning requires vast processing resources.

There are two main disadvantages associated with content filtering software. The first is an inability to adequately block inappropriate images. Lack of image scanning often results in partial loading of a web page containing inappropriate content before a prohibited word or phrase is encountered, resulting in viewing of inappropriate content. The other drawback to content scanning is that it is difficult to determine words or phrases to base scanning upon in order to filter out certain topics, such as drugs or violence. For example, a

web page describing how to make a narcotic may contain only chemical formulas and not describe the drug itself in words or phrases that the content scanning software recognizes.

Problems common to both site blocking software and content scanning software also exist. For example, both are difficult to implement across different platforms, i.e., it is difficult to transport the software from one operating system to another. Also, the settings from either form of software apply only to the local computer, or at best to a local network, on which a particular copy of the software is installed, resulting in protection only at the computer where the particular copy is installed and not everywhere a user might access the Internet from. This lack of consistent filtering exists, even if another computer is running the same filtering software, but does not utilize the same configurations.

Many attempts to create a robust filtering program have been made. Six popular Internet content filtering programs are described by PC Magazine's April 18, 2000 edition on the ZDNet web site (http://www.zdnet.com/products/stories/reviews/0,4161,2537795,00.html) as follows:

BAIR Filtering System™, Version 3.2.1 detects pornographic images and text, but does not include other text filters, block outgoing content, block features such as chat and instant messages, block access to blacklisted sites, restrict access to listed safe sites, log activity or violations, limit time on the Internet, or have an operating mode that is undetectable by users.

Cyber Sentinel™ 2.0 detects pornographic text, blocks outgoing content, blocks features such as chat and instant messages, blocks access to blacklisted sites, restricts access to listed safe sites, logs activity or violations, limits time on the Internet, and has an operating mode that is undetectable by users, but does not detect pornographic images or include text filters other than pornography filters.

Cyber Sitter 2000™ detects pornographic text, includes text filters other than pornography filters, blocks outgoing content, blocks features such as chat and instant messages, blocks access to blacklisted sites, logs activity or violations, limits time on the Internet, and has an operating mode that is undetectable by users, but does not detect pornographic images or restrict access to listed safe sites.

Eyeguard™ 1.02 detects pornographic images and logs activity or violations, but does not detect pornographic or other text, block outgoing content, block features such as chat and instant messages, block access to blacklisted sites, restrict access to listed safe sites, limit time on the Internet, or have an operating mode that is undetectable by users.

SOS KidProof™ 1.65 detects pornographic text, blocks access to blacklisted sites, restricts access to listed safe sites, logs activity or violations, and limits time on the Internet, but does not detect pornographic images, include text filters other than pornography filters, block outgoing content, block features such as chat and instant messages, or have an operating mode that is undetectable by users.

X-Stop™ 3.04 detects pornographic text, blocks outgoing content, and blocks access to blacklisted sites, but does not detect pornographic images, include text filters other than pornography filters, block features such as chat and instant messages, restrict access to listed safe sites, log activity or violations, limit time on the Internet, or have an operating mode that is undetectable by users.

Although four of the six programs combine site blocking and content filtering, none of the programs utilizing site blocking provide a robust, automated manner for keeping blocked site lists updated with new sites on the Internet. It is also especially important to note that no program provides consistent filtering, i.e., a roaming user profile, when a user accesses the WWW from different computers, and that all programs are designed primarily for home use.

It should also be noted that the BAIR™ approach to image recognition is performed on a bank of Cray™ supercomputers. See PC Magazine's review in the April 18, 2000 edition, reprinted by ZDNet at http://www.zdnet.com/products/stories/pipreviews/0,8827,195175,00.html. Although use of Cray™ supercomputers allows BAIR™ to utilize a high level of processor capability, the BAIR™ approach is limited by centralization of all the filtering functions in one location. Such centralization leads to an eventual overload on even Cray™ supercomputers because of the exponentially increasing demand for processing power required by a linearly increasing number of subscribers.

Often, utilizing software designed for home use in an academic environment is administratively complex, expensive and unreliable in that it leads to either over-inclusive or under-inclusive filtering. Over-inclusive and under-inclusive filtering occurs because school administrators have little or no idea of what material different parents consider appropriate for their children, resulting in the level of filtering being too strict for some parents' tolerance for what their children may view, and at the same time being too relaxed for other parents' tolerance for what their children may view.

Accordingly, there remains a need for a comprehensive solution for consistent Internet filtering when access to the Internet is made from various computer systems. A

particular need exists for a filter solution allowing parents to control what level of filtering applies to their child, while using the Internet at school, without the attendant disadvantages of conventionally available site blocking and/or content filtering/scanning software and methods.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide limited access to Internet content by filtering out material deemed inappropriate for a child by a parent or guardian of the child.

It is another object of the present invention to provide a consistent level of filtering for a child no matter where the child accesses the Internet from, for example, if the child accesses the Internet from a school, a public library, or at home.

The above and other objects are accomplished by distributing Internet filtering software between access control servers connected to the Internet and local computer systems, and by logging Internet sites accessed by children.

To accomplish the above and other objects, the present invention provides Internet access control servers running a portion of an Internet filtering software. Local computer systems run a second portion of the Internet filtering software. The filter functions preferably include both site blocking and content filtering. The invention envisions coordinating both portions of the Internet filtering software to distribute tasks in a client/server manner between access control servers (servers) and local computer systems (clients), and to enable access control servers to learn new, inappropriate sites from local computer systems. The central server also transfers individualized configurations or profiles to the client computers as users access the Internet from different computers, to give each user a uniform filtering regardless of the access point.

Accordingly, one aspect of the invention relates to granting access to Internet content utilizing a computer system and an internet server by transmitting a Uniform Resource Locator (URL) associated with Internet content and an identifier associated with a user of the computer system to an Internet server. The Internet server determines whether the user is to be granted access to the Internet content by checking a database containing permitted URLs and prohibited URLs and bases the determination upon access parameters associated with the user's identifier. The transmitted URL is then logged in association with the user's identifier. If the user is not granted access to the URL then the user's computer system displays an appropriate message. However, if the user is granted access to the

BNSDOCID: <WO___0198934A2_I_>

URL, then the Internet content associated with the URL is downloaded onto the user's computer system. The user's computer system scans the content, as it is downloaded, to determine if one or more predetermined words or phrases are present in the Internet content. If one or more predetermined words or phrases are present in the Internet content, then the download of the Internet content to the user's computer system is terminated, and the URL associated with the Internet content is logged as a prohibited URL in the database. (See comment re claim 1).

Another aspect of the invention relates to granting access to Internet content utilizing a computer system by transmitting a Uniform Resource Locator (URL) associated with Internet content and an identifier associated with a user of a computer system. Information whether access is granted or denied is received and the URL is logged in association with the user's identifier. If access is not granted then the computer system displays an appropriate message. However, if access is granted, then the computer system downloads the Internet content associated with the URL and scans the content as it is downloaded to determine whether predetermined words or phrases are present. If one or more predetermined words or phrases are present, the download is terminated and the URL is transmitted. Accordingly, yet another aspect of the invention relates to granting access to Internet content utilizing an internet server by receiving a Uniform Resource Locator (URL) associated with Internet content and an identifier associated with a computer user, and determining whether the user is to be granted access to the URL by checking a database containing permitted URLs and prohibited URLs based upon access parameters associated with the user's identifier. Whether the user is granted or denied access is transmitted, and information concerning the scanned internet content associated with the URL is received if access was granted. If granted, the user's computer scans content during downloading. If one or more predetermined words or phrases is present in the scanned internet content the associated URL is logged in the database as a prohibited URL. Finally, a list of URLs accessed by the user is transmitted.

The methods of the present invention may be employed in any suitable conventional manner, e.g., via the use of a computer and server communicating via the public data network commonly known as the Internet.

Essentially, the server provides a centralized resource for site blocking functionality. The user computers, however, perform content filtering and update the database of prohibited URLs maintained at the server, based on the results of the local scanning

performed during content filtering. Stated another way, each user's computer becomes a resource for reviewing internet content and updating the URL database.

The central server also stores user profile data, and downloads the latest updated version of a user's profile to the terminal computer each time that a particular user accesses the Internet. The server provides the same profile for a given user, to each different terminal computer from which that user logs-in. The user's profile for site blocking and the URL database are uniformly maintained and implemented at the internet server, and the downloading of profiles to terminal computers at time of access provides a uniform application of each user's profile for content scanning and filtering across multiple access platforms.

In addition to the inventive methods, other aspects of the invention relate to a computer system and/or a server executing the distributed filtering software. Still further aspects of the invention relate to the software products themselves.

Additional aspects, embodiments and advantages of the present invention will be set forth, in part, in the description that follows, or may be learned from practicing or using the present invention. The objects and advantages may be realized and attained by means of the features and combinations particularly pointed out throughout this description and the appended claims. It is to be understood that the foregoing general description and the following detailed description are exemplary and explanatory only and are not to be viewed as being restrictive of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the present invention and, together with the description, serve to exemplify the principles of the present invention.

Fig. 1 shows an embodiment of a client/server topology utilized with the present invention.

Fig. 2 shows an exemplary transaction carried out over the topology depicted in Figure 1.

Fig. 3 shows a configuration window utilized with an embodiment of client software for the present invention utilized to implement the transaction depicted in Figure 2.

Fig. 4 shows a time management window utilized with the embodiment of client software for the present invention as shown in Figure 2a.

BNSDOCID: <WO___0198934A2_I_>

Fig. 5 shows a system window utilized with the embodiment of client software for the present invention as shown in Figure 2a.

Fig. 6 shows a processing flow for starting client software of an embodiment of the present invention.

Fig. 7 shows a logout procedure for the embodiment shown in Figure 6.

Fig. 8 shows a processing flow for enabling and disabling the embodiment of the present invention depicted in Figure 6.

Fig. 9 shows a service login procedure for the embodiment of the present invention shown in Figure 6.

Fig. 10 shows a processing flow for starting a browser helper object utilized with the embodiment of the present invention depicted in Figure 6.

Fig. 11 shows a processing flow for content filtering and for learning and blocking Universal Resource Locators according to the embodiment depicted in Figure 6.

Fig. 12 shows a processing flow for a Universal Resource Locator request procedure in accordance with the embodiment depicted in Figure 6.

Fig. 13 shows a redirection procedure performed by an access control server according to the embodiment depicted in Figure 6.

Fig. 14 shows a process flow for a queue scheduling procedure in accordance with the embodiment depicted in Figure 6.

Fig. 15 shows a process flow for reviewing a web site associated with a requested Uniform Resource Locator in accordance with the embodiment depicted in Figure 6.

Fig. 16 shows an exemplary user table and associated fields utilized with the embodiment of the present invention depicted Figure 6.

Fig. 17 shows an exemplary approved Universal Resource Locator table and associated fields utilized with the embodiment of the present invention depicted Figure 6.

Fig. 18 shows an exemplary blocked Universal Resource Locator table and associated fields utilized with the embodiment of the present invention depicted Figure 6.

Fig. 19 shows a computer system capable of implementing the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The Internet is a vast resource that provides fast, easy access to an almost limitless variety of information. Information contained on the Internet is useful for academics, work, and research and enhances people's ability to learn. However, not every use of the Internet

is appropriate for all settings and it is therefore desirable to limit what content certain groups of Internet users can access during specified times and/or from specified locations. The present invention provides an efficient and novel apparatus and method for restricting access to Internet content wherein a parent or guardian defines what level of filtering of Internet content is appropriate for their child, and the parentally defined level of filtering applies whether the child is accessing the Internet from home, school, or another location.

When a parent utilizes the client software of the present invention to define what Internet content their child may access, the information is stored as a child's profile in a database communicating with an Internet server. The Internet server then acts as an access control server by handling requests by the child for Internet content. Because a child's profile is stored by a remote Internet server, whenever the child accesses the Internet from a computer system running the client software, no matter where that computer system is located and regardless of the particular copy of the client software that the computer system is running, the child's access to the Internet is governed by the same profile established by the child's parents. Utilization of the same profile for the child is possible because each client software redirects Internet content requests to the access control server so that the child's profile may be looked up from the database and used to control the Internet content that is delivered to the child. The server uniformly applies the profile for site blocking type functions. The user computer receives at least a portion of the profile during each access, so that each computer the child uses applies the same constraints for content scanning and filtering functions.

SOFTWARE OVERVIEW

Referring to Figure 1, topology of an exemplary embodiment, is depicted. The exemplary software comprises two components that share Internet content filtering processing, a client component and a server component. Throughout this description, the term "Internet content" shall mean, without limitation, text, graphics, audio, video, chat, streaming audio, streaming video, internet radio, internet television, and the like. The client component, described in detail infra, is loaded onto each client computer system 100, and runs locally on each computer system 100, which can be a stand-alone computer, or part of a network of computers. Computer system 100 is typically a home computer system, a school computer system, or part of a library computer system. The server component of the exemplary software, described in detail infra, is loaded onto an Internet access control server 115 and communicates with the client software running on computer system 100.

BNSDOCID: <WO___0198934A2_I_>

Processing tasks are divided between the client and the server. For example, the client handles the logon procedure; performs real time content filtering; learns from content filtering and causes Uniform Resource Locators ("URLs") to be blocked to be stored in a remote database 120; enables and disables the filtering software; caches the last logon for use if the server cannot be reached at a subsequent logon; redirects URL requests through an access control server; retrieves user profiles from an access control server; logs access on the local computer system 100 as well as web sites accessed; and updates local software files as needed. URL requests include hypertext transfer protocol (HTTP), standard generalized markup language (SGML), which is a system for organizing and tagging elements of a document encompassing the hypertext markup language (HTML) and the extensible markup language (XML), as well as emerging protocols. Tasks performed by the server software include; controlling actual access to web sites responsive to the redirected URL requests; recording access to web sites for data mining purposes; storing a configuration for each individual user as well as other user information; scanning web sites for inclusion into allowed or prohibited lists; allowing parents or guardians to view information about what web sites their child or ward has accessed; storing user profiles and passing user profiles to the client; and storing files used to update clients when the clients are connected to the server.

The client software is capable of being disabled or enabled after it is loaded onto computer system 100. If the client is disabled, then any request for Internet content, typically utilizing a Uniform Resource Locator ("URL"), issuing from a browser running on computer system 100 is sent directly to the Internet 105, and the Internet content is returned unfiltered. However, if the client is enabled, then it cooperates with the server software to provide comprehensive filtering of requests for Internet content and of the returned Internet content, if any.

Cooperation between the client and the server is accomplished in several manners. For example, when a parent installs the client on a computer system 100, the parent must configure the filter settings that will be used when the parent's child access the Internet 105. The configuration process establishes communication from computer system 100, through firewall 110 to access server 115, and causes the parentally defined filter configuration to be stored on database 120, along with an identifier that identifies what child to match the filter configuration with. Storing a child's Internet filter configuration on database 120 permits the server software, running on access control server 115, to provide the same level of filtering of Internet content for the same child whenever the child accesses the Internet 105 using

computer system 100, or any computer system (not shown) running the client software no matter where the computer system is located, as explained in detail infra.

Another example of cooperation is the distribution of filtering processes between the server and the client. The server performs checks by comparing a requested URL against a list of prohibited URLs and against a list of allowed URLs to determine whether the requested URL is one that can be accessed by a particular child. When Internet content associated with a URL is transmitted from the Internet 105 to computer system 100, the client performs a scan of the incoming content to determine whether the content is appropriate in light of the filter configuration specified for the child.

By distributing processing between access control servers 115 and local computer systems 100, the present invention reduces the processing load at any one point, thereby increasing the speed at which filtering is performed and reducing the need to constantly add expensive upgrades to access control servers 115 and to add new access control servers 115. By centralizing certain control functions in the access control server, the invention provides uniform control regardless of which computer 100 a child uses at any particular time.

When computer system 100 is booted, and the client is enabled, a user, typically a child, must logon to the client before any requests for content from the Internet 105 can be made. If the client is set up in single user mode, then logon to the client can be set to be automatic when computer system 100 is booted. However, the client also has a multiple user mode that requires a child to enter a username and password in order to logon to the client. A child may logon to the client when computer system 100 is booted, or the child may wait until an Internet browser is started to logon to the client. Because the client comprises a browser helper object, a program that attaches to and becomes a part of a browser, when the client is enabled, it controls the operation of a browser. This browser control includes forbidding the browser to transmit a request for Internet content unless a child has logged-on to the client.

Once a browser has been started on computer system 100, and a child has logged-on to the enabled client, a request for Internet content, typically in the form of a Universal Resource Locator ("URL"), can be sent from computer system 100. However, unlike when the client is disabled, the initial request for Internet content is not sent directly to the Internet 105, but is redirected through firewall 110 to an access control server 115. The initial request for access to a URL associated with Internet content is also accompanied with an identifier, i.e., the child's username, when the initial request is redirected to an access

BNSDOCID: <WO___0198934A2_I_>

control server 115. Including the child's identifier allows access control server 115 to perform a database query on database 120 to look-up the Internet filter configuration that the child's parents have established. By controlling a browser to redirect URL requests to an access server 115 where a child's filter configuration is looked-up, the same level of filtering of Internet content whenever the child accesses the Internet 105 is possible. As long as the computer system 100 is running the client the child receives the same level of filtering of Internet content regardless of whether computer system 100 is the child's home computer system, a computer system at the child's school, a computer system at a public library, or other computer system. The same level of Internet content filtering is possible because the filter configuration for each child is stored on a database 120 accessible by an Internet server, i.e., access control server 115, and is used for every Internet session, no matter where a child accesses the Internet from. The type of content filtered encompasses text, graphics, audio, video, chat, streaming audio, streaming video, internet radio, internet television, etc.

Not only does a parent define what categories of content are appropriate for their child when establishing the filter configuration for their child, but a parent also defines how filtering is to occur. The server utilizes a list of prohibited URLs and a list of approved URLs, typically stored on database 120, to determine whether a particular child has access to a requested URL. The child's parents define how an access control server 115 utilizes the prohibited list and the approved list when determining access to a requested URL.

One possibility is to specify that only URLs on the approved list may be accessed by the child. Permitting access only to URLs on the allowed list causes an access control server 115 to compare a requested URL against the allowed list, table 1700 (Figure 17). If the requested URL is not found on the allowed list 1700, then the child is redirected to an access denied page (not shown). However, if the requested URL is found on the allowed list 1700, then the access control server 115 redirects the child's URL request to the Internet 105 where the content associated with the requested URL is retrieved, then transmitted to computer system 100. Further filtering may occur using the access field 1702 associated with a URL field 1704. For example, a requested URL might only be allowable to children whose parents have selected a predefined level of access. If a child does not have the level required for a URL field 1704 as defined by an associated access field 1702, then the child is sent to an access denied page. To reduce processing time, the computer system 100 might not perform a scan of the incoming content (because it is from a known, approved URL) for predetermined words and/or phrases. However, a parent could specify in the

BNSDOCID: <WO___0198934A2_I_>

child's filter configuration that computer system 100 should always perform a scan for predetermined words and/or phrases. Parents are able to modify the list of words and phrases used during scanning of Internet content for their child by modifying a child's profile, discussed in detail infra. If computer system 100 performs a scan for predetermined words and/or phrases, and a predetermined word and/or phrase is found in the incoming content, downloading the web page associated with the requested URL is stopped, and notification is transmitted to access control server 115 to place the requested URL on the prohibited list and to remove it from the allowed list. Alternatively, the access level associated with the URL cold be changed to a higher level. A predetermined word and/or phrase might be found on incoming content associated with an allowed URL, for example, if the content of the web page associated with the URL is changed without changing the URL itself.

Another possibility is to specify that URLs on the prohibited list may not be accessed, but any URL not on the prohibited list may be accessed. Permitting access to URLs not on the prohibited list causes an access control server 115 to compare the requested URL against the list of prohibited URLs, table 1800 (Figure 18). If the requested URL is found on the prohibited list 1800, then the child is redirected to an access denied page (not shown). As with the allowed list 1700, each URL 1804 on the prohibited list 1800 can be associated with an access level 1802 that acts as a further filter requirement, depending upon a child's parentally defined access level. However, if the requested URL is not found on the prohibited list 1800, then regardless of whether the requested URL is on the allowed list 1700, the child's request is redirected to the Internet 105 where the content associated with the requested URL is retrieved and transmitted to computer system 100 as described supra.

A third possibility is to specify that a child may access URLs on the allowed list 1700, but if a requested URL is not on the allowed list 1700, nor on the prohibited list 1800, then a check is performed before the child is granted or denied access to the requested URL. When a child requests a URL, and that requested URL is not on the allowed list 1700 or on the prohibited list 1800, an access control server 115 sends a message to the child indicating that the requested URL must be checked. The access control server 115 then submits the requested URL to a checker process, described in detail below, to determine whether the child may access the URL. The checker utilizes the same content scanning process that computer system 100 employs, and then classifies the requested URL for placement either onto the allowed list 1700 or onto the prohibited list 1800. When the child requests the URL again, access control server 115 locates the URL on either the allowed list 1700 or on the prohibited list 1800 and grants or denies access accordingly.

BNSDOCID: <WO___0198934A2_I_>

HARDWARE OVERVIEW

Figure 19 is a block diagram that illustrates a computer system 100 upon which an embodiment of the invention may be implemented. Computer system 100 includes a bus 1902 or other communication mechanism for communicating information, and a processor 1904 coupled with bus 1902 for processing information. Computer system 100 also includes a main memory 1906, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 1902 for storing information and instructions to be executed by processor 1904. Main memory 1906 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 1904. Computer system 100 further includes a read only memory (ROM) 1908 or other static storage device coupled to bus 1902 for storing static information and instructions for processor 1904. A storage device 1910, such as a magnetic disk or optical disk, is provided and coupled to bus 1902 for storing information and instructions.

Computer system 100 may be coupled via bus 1902 to a display 1912, such as a cathode ray tube (CRT), for displaying information to a computer user. An input device 1914, including alphanumeric and other keys, is coupled to bus 1902 for communicating information and command selections to processor 1904. Another type of user input device is cursor control 1916, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 1904 and for controlling cursor movement on display 1912. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify positions in a plane.

The invention is related to the use of computer system 100 for filtering Internet content in conjunction with an Internet server 115. According to certain embodiments of the invention, filtering of Internet content is provided partially by computer system 100 in response to processor 1904 executing one or more sequences of one or more instructions contained in main memory 1906. Such instructions, for example the client may be read into main memory 1906 from another computer-readable medium, such as storage device 1910. Execution of the sequences of instructions contained in main memory 1906 causes processor 1904 to perform the process steps described herein. One or more processors in a multi-processing arrangement may also be employed to execute the sequences of instructions contained in main memory 1906. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement

the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 1904 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as storage device 1910. Volatile media include dynamic memory, such as main memory 1906. Transmission media include coaxial cables, copper wire and fiber optics, including the wires that comprise bus 1902. Transmission media can also take the form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 1904 for execution. For example, the instructions may initially be borne on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 100 can receive the data on the telephone line and use an infrared transmitter to convert the data to an infrared signal. An infrared detector coupled to bus 1902 can receive the data carried in the infrared signal and place the data on bus 1902. Bus 1902 carries the data to main memory 1906, from which processor 1904 retrieves and executes the instructions. The instructions received by main memory 1906 may optionally be stored on storage device 1910 either before or after execution by processor 1904.

Computer system 100 also includes a communication interface 1918 coupled to bus 1902. Communication interface 1918 provides a two-way data communication coupling to a network link 1920 that is connected to a local network 1922. For example, communication interface 1918 may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 1918 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be

implemented. In any such implementation, communication interface 1918 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

Network link 1920 typically provides data communication through one or more networks to other data devices. For example, network link 1920 may provide a connection through local network 1922 to a host computer 1924 or to data equipment operated by an Internet Service Provider (ISP) 1926. ISP 1926 in turn provides data communication services through the worldwide packet data communication network, now commonly referred to as the "Internet" 105. Local network 1922 and Internet 105 both use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 1920 and through communication interface 1918, which carry the digital data to and from computer system 100, are exemplary forms of carrier waves transporting the information.

Computer system 100 can send messages and receive data, including program code, through the network(s), network link 1920, and communication interface 1918. In the Internet example, an access control server 115 might transmit a requested URL after the access control server 115 has checked the URL against both an allowed table 1700 and a prohibited table 1800 over Internet 105, ISP 1926, local network 1922 and communication interface 1918. In accordance with the invention, one such transaction provides for filtering of Internet content by both an access control server 115 and by a local computer system 100.

The present invention may be embodied in a computer system as described above, or it may be a program designed to operate on any configuration for a computer system.

EXEMPLARY TRANSACTION UTILIZING CLIENT AND SERVER SOFTWARE

An exemplary transaction is described, referencing Figures 2-15.

Figure 2 depicts a client computer system 100 communicating with an Internet access control server 115, which in turn communicates with a data base 120, an access denied web page 200, and a plurality of internet servers 205 (only one is shown for clarity). When a child boots computer system 100, and desires to access the internet, he may either logon to the client, or start a web browser residing on computer system 100. Whether the child chooses to logon to the client first, or start the internet browser first, the child is prompted to logon to the client at some point.

BNSDOCID: <WO___0198934A2_I_>

Figure 6 depicts the processing flow when the client is started. The client is started at step 600 when computer system 100 is booted, and a login variable is initializes to "False" at step 605. At step 610, the client loads settings that are stored locally on computer system 100. Examples of locally stored settings are depicted in Figures 3-5, which show windows accessible only by someone who knows the master password for the local client running on computer system 100.

Figure 3 depicts a configuration window used when administering the client. Clicking on the "Configure a user" icon allows a parent or guardian to specify the filter configurations that apply to a child's Internet sessions. Exemplary filter configurations include what content the child is allowed, or is not allowed, to access (selected from various categories such as sexually explicit, violence, racial, etc.), how scanning is to be performed by an access control server 115, how filtering is to be performed by computer system 100, and what words and/or phrases are to be used by the local computer system when scanning for content. Clicking on the "View a user's activity" icon allows a parent to view a list of URLs that a particular child has visited by entering the child's identifier. The access control server 115 then retrieves and displays a list of web sites, and/or associated URLs, that the child has accessed. Clicking on the "Create a new user" icon allows a parent to establish a new account, i.e., establish a unique identifier, for a child to use with the client and server software. Clicking on the "Change the password" icon allows a parent to change the master password for the client running on computer system 100. Clicking on the "View local activity" icon allows a parent to view a display of activity that a child has engaged in on the local computer system 100. Local activity on computer system 100, such as an attempted change of the client's master password, is logged by the client and can later be viewed. Checking the "Auto login" check box and entering a user account, i.e., a child's username, allows a parent to set the client to automatically login the specified child when computer system 100 is booted. Not checking the "Auto login" check box enables the client to receive logon information from a logon window relating to different children using computer system 100. Checking the "Allow guest user" check box enables children who do not have a profile stored on the server to access the Internet from computer system 100. A default filter configuration is utilized for children who do not have a profile stored on the server. For example, the default can be very protective and be set to allow access only to URLs on the allowed list, and to perform content scanning by computer system 100 on all content downloaded from the Internet 105. Checking the "Log user activity" check box instructs an access control server 115 to keep a log of URLs that children using computer system 100 to

BNSDOCID: <WO___0198934A2_I_>

access the Internet. Such an access log is then used to display URLs and/or associated web pages if a parent clicks on the "View a user's activity" icon.

Figure 4 depicts a Time management window used to control when a child using computer system 100 may access the Internet 105. For each day of the week, clicking on a block (which represents an hour) toggles the block between access allowed and access denied. By toggling each block to the desired setting, a parent configures the client regarding the time of day when a child may access the Internet for each day of the week.

Figure 5 depicts a System window used to control what features on the local computer system 100 a child can access. Checking a check box next to a feature makes that feature unavailable to a child using computer system 100, while a blank check box indicates that children may access the feature. For example, in Figure 5 a child using computer system 100 would not be able to access the 'Control Panel' (on Microsoft Windows™), but would be able to access the 'Printers' folder (on Microsoft Windows™).

Referring again to Figure 6, an icon related to the exemplary embodiment of the invention is added to the display on computer system 100 at step 615. For example, if the computer system 100 is running Microsoft Windows™, then the icon related to the exemplary embodiment of the invention is added to the tray in the lower right-hand corner of the screen. A determination is then made at step 620 to verify whether the automatic login feature, see Figure 3, is enabled. If the automatic login feature is enabled, then the client stores the user account entered in the Configuration window (Figure 3). If the automatic login feature is not enabled, then a login dialog window is displayed at step 625. A user may enter a user account into the login dialog window, and the client stores the entered user account. However, if the user ignores the login dialog window, the login dialog window simply remains on the display and is hidden behind other windows when the user utilizes other programs on computer system 100. The client is then set to the enabled mode at step 630, and a check is performed at step 635 to determine whether there are new versions of updateable files for the client. The check at step 635 access a database 120 via an access control server 115, and downloads new files from database 120 if there are new files to download.

Clicking on the icon, added to the display for computer system 100 in step 615, presents several options. One option is to logout of the client, while another option is to enable or disable the client.

After the icon has been clicked, referring to Figure 7, a user selects to logout at step 700. The login variable is set to "False" at step 705, and any user profile stored in random

access memory is cleared at step 710. A check is performed at step 715 to determine whether the client is configured for automatic login. If automatic login is enabled, then the user account stored, refer to Figure 3, is used to login to the client and the logout procedure ends at step 725. If automatic login is not enabled, then a login dialog window is displayed at step 720, and processing ends at step 725 if no user account information is entered into the login dialog window.

After clicking on the icon related to the exemplary embodiment of the invention, referring to Figure 8, a user may enable or disable the client, starting at step 800. If a user desires to enable the client at step 805, processing simply continues to step 825 where the client is enabled. However, if a user desires to disable the client at step 805, then processing proceeds to step 810 where the user is prompted to enter the master password for the client. The entered password is compared to the master password at step 815. If the entered password does not match the master password, then processing ends at step 830. If the entered password matches the master password, then the client is disabled at step 820. Disabling the client allows a parent to use computer system 100 to access the Internet 105 without filtering the content received from the Internet 105.

When a browser is started on computer system 100, the client starts a browser helper object as depicted in Figure 10. At step 1000 the browser helper object ("BHO") is started and attaches to a browser, for example via a hook proc for Microsoft Internet Explorer. The BHO determines whether the client is enabled at step 1005. If the BHO determines that the client is disabled, then processing ends at step 1025 and the browser is used to access the Internet 105 without any filtering of Internet content occurring. However, if the BHO determines that the client is enabled at step 1005, then processing continues at step 1010 where the BHO determines whether a user has already logged-on to the client. If a user has logged-on to the client, then processing continues at step 1020 where the BHO utilizes the user account information stored by the client to logon to an access control server 115. If a user is not already logged-in to the client, then a determination is made at step 1015 whether the automatic login feature is enabled. Regardless of whether the automatic login feature is enabled, processing continues at step 1020. However, if automatic login is enabled, then the BHO utilizes the user account information entered on the Configuration window (see Figure 3) to logon to an access control server 115. If automatic login is not enabled, then the BHO does not utilize any account information, which signifies a guest user, to logon to an access control server 115.

BNSDOCID: <WO___0198934A2_I_>

Referring to Figure 9, the service logon (step 1020 in Figure 10) to an access control server 115 starts at step 900. At step 902 a determination is made whether an automatic login was made to the client. If an automatic login to the client was made, then the username value is set to correspond to the user account entered in the Configuration window (Figure 3) at step 906. If an automatic login to the client was not made, a determination is made at step 904 whether the login to the client is a guest login. If the login is not a guest login, then the username value is set to correspond to the user account entered in the login dialog window at step 908.

If the login is a guest login, then the username value is left blank at step 910. A profile is then retrieved at step 912 from an access server 115 using the set username value. Exemplary information contained in the retrieved profile includes child information, such as last name, address, etc., that the parent has designated as not to be sent out over the Internet, as well as an exclusion list of URLs that the child may not access. A determination is then made at step 914 whether the username, and therefore the profile, is valid, i.e., does the child have a profile stored on the server or is the username the guest username? If the username is not valid, then a determination is made at step 916 whether the login was automatic. If the login was not automatic, then the values entered into the login dialog box are cleared at step 918, and an error message is displayed at step 924 indicating that the user account information entered was not valid.

If the login was automatic, then the automatic login feature is disabled at step 920, and a login dialog window is displayed at step 922. Concurrently with opening a login dialog window, an error message indicating that the automatic login feature contains invalid user account information is displayed at step 924. When an invalid username is discovered, a user must then enter their account information, i.e., username and password, and the service login procedure restarts at step 900.

If the username is valid, then a determination is made at step 926 whether login was automatic. If login was automatic, then the login is cached at step 932. If the login was not automatic, then a determination is made at step 928 whether the password entered matches the password associated with the username and stored in the database 120. If the entered password matches the stored password, then the login dialog window is closed at step 930, and the login is cached at step 932. If the entered password does not match the stored password, then the values in the login dialog window are cleared at step 934, and an error message indicating that the user account information is not valid is displayed at step 938. After the login has been cached at step 932, the retrieved profile is stored in memory at step

936. The profile can be stored in random access memory, or on computer system 100's hard drive, depending upon design considerations. After the profile has been stored in memory, the login variable is set to "True" at step 940 and the BHO is logged-on to an access control server 115.

After a browser has started on computer system 100 and the BHO has logged-on to an access control server 115, a child can request a URL from the Internet 105. In Figure 12, step 1200 represents selection of a URL and transmission of the requested URL. At step 1205, a determination is made whether the client is enabled on the local computer system 100. If the client is not enabled, then processing continues at step 1210 where the URL request is sent directly to the Internet 105 and Internet content is retrieved without any filtering occurring.

If the client is enabled, then a determination is made at step 1215 whether the BHO is logged-in to an access control server 115. If the BHO is not logged-in, then processing continues at step 1225 where a determination is made whether the automatic login feature is enabled. If the automatic login feature is enabled, BHO login occurs as described in relation to Figure 9, supra. A determination is then made at step 1235 whether the automatic service login was successful. However, if the automatic login feature is determined to be disabled in step 1225, or a determination is made at step 1235 that the service login did not occur, then access is blocked at step 1265. An error message is displayed at step 1270 indicating that the user must login to the client before access to the Internet 105 can be granted. The user must then logon as depicted in Figure 9 before access to the Internet will be granted.

After assuring that the BHO is logged-in to an access control server 115 at step 1235, a determination is made at step 1220 whether the requested URL is being loaded in a frame. The determination at step 1220 is made in order to prevent sending a requested URL that is loaded within a web page designated by another URL to an access control server 115. If it is determined that the requested URL is loaded in a frame, then the requested URL is downloaded in a normal manner at step 1245 onto computer system 100. If it is determined that the requested URL is not loaded in a frame, i.e., is not contained within another web page, then a determination is made at step 1240 whether the requested URL is in the exclusion list downloaded as part of the profile in step 912 of Figure 9.

If the URL requested is in the downloaded exclusion list, then the requested URL is downloaded in a normal manner onto computer system 100 at step 1245. If the requested URL is not in the downloaded exclusion list, then the requested URL is redirected through

BNSDOCID: <WO___0198934A2_I_>

an access control server 115 at step 1250, where the requested URL is checked against a comprehensive exclusion list residing on database 120. Redirecting a requested URL through an access control server 115 is described in detail infra, referring to Figure 13. After a requested URL is either loaded normally at step 1245, or is returned from an access control server 115 from step 1250, a determination is made at step 1255 whether the requested URL was on any exclusion list. If the requested URL was found on an exclusion list, then the user will not see the content associated with the requested URL and processing ends at step 1275. If the requested URL was not found on an exclusion list, then the BHO conducts a content filter of the material associated with the requested URL, as described in detail infra referring to Figure 11.

Redirecting a requested URL through an access control server (step 1250 in Figure 12) occurs when the requested URL is not on the exclusion list downloaded as part of a user's profile, step 912 in Figure 9. Referring to Figure 13, when a requested URL is redirected through an access control server 115, the processing flow starts at step 1300, when a URL and an identifier, i.e., a user name, are received. At step 1305 a determination is made whether a URL was passed to the access control server 115. If no URL was passed to the access control server 115, the user is redirected to an access denied page at step 1330 and processing ends at step 1395.

If a URL was passed, then a determination is made whether a user name was also passed at step 1310. If no user name was passed, then step 1315 assumes that a guest user account is being used, and the username is set to guest. At step 1320, the username is looked up in the database 120. At step 1325 a determination is made whether the username was found. If no username was found in the database 120, the user is redirected to an access denied page at step 1330, and processing ends at step 1395.

A protection mode, defining how filtering is to occur and what level of filtering is applied, is associated with each username and stored in database 120. Protection modes are defined by parents or guardians when children's accounts are established. If the username was found in the database 120, the protection mode is retrieved at step 1335. At step 1340 a determination is made of what mode, either exclusive or blocking, is associated with the username. For blocking mode, processing continues at step 1345 where the requested URL information is looked up in the database 120. A determination is made at step 1350 whether the requested URL should be blocked based upon the result of the information retrieved from step 1345. If the requested URL should be blocked, the user is redirected to an access denied page at step 1355, and processing ends at step 1395. If the

BNSDOCID: <WO___0198934A2_I_>

requested URL is not blocked, then processing continues at step 1370 where a determination is made whether a verification has been made pursuant to the Children Online Privacy Protection Act (COPPA). If a COPPA verification has been made, then the user's access to the requested URL is logged onto the remote access control server 115 and stored in the database 120 at step 1375. If no COPPA verification has been made, then the user is redirected to the URL that they requested at step 1380. If the mode determined in step 1340 is exclusive, then processing continues at step 1360 where the requested URL information is looked up in the database 120. At step 1365 a determination is made whether the requested URL is allowed based upon the result of the information retrieved from step 1360. If the requested URL is allowed, then processing continues at step 1370 as described supra. If the requested URL is not allowed, then processing continues at step 1385 where the requested URL is added to a check table to be later checked for content. Then, the user is redirected to an access denied page at step 1390 and the user is informed that the requested URL will be checked.

The process of checking a URL by an access control server 115 is described referring to Figures 14 and 15. Figure 14 depicts the process flow for scheduling a review of a requested URL. At step 1405 a determination is made whether any new URLs are in the check table residing in database 120. A new URL is added to the check table as a result of step 1385 in Figure 13. If no new URLs are in the check table, then processing ends at step 1440. If there is a new URL in the check table, then a determination is made whether the URL is already in the database 120 at step 1410. If the URL is already in the database 120, processing ends at step 1440. If the URL is not already in the database 120, a determination is made whether a checker process is already running at step 1415. If there are no checker processes running, a new process is launched at step 1425 and the URL is added to the queue for the new checker process. If checker processes are already running, then a determination is made at step 1420 whether all processes are operating at full capacity. If all checker processes are operating at full capacity, a new checker process is launched at step 1425 and the URL is added to the queue for the new checker process. If all running checker processes are not operating at full capacity at step 1420, then the checker process with the least amount of URLs to scan is identified in step 1430. The URL to be checked is then added to the checker process with the least amount of URLs to scan at step 1435.

The checker reviewing procedure is depicted in Figure 15. At step 1505 a determination is made whether there are any URLs in the queue for the checker process to

BNSDOCID: <WO___0198934A2_I_>

check. If there are no URLs in the checker's queue, then processing ends at step 1545. If there is a URL to be checked, then processing continues at step 1510 where the web page associated with the URL is downloaded. The content on the downloaded web page is checked at step 1515 by scanning all of the words on the web page. At step 1520 a determination is made whether the content is inappropriate or not by comparing the scanned words to a predetermined list of words and phrases. If the content is inappropriate, i.e., a match is found with at least one of the predetermined words or phrases, then the URL is added to the block list on the database 120 at step 1525. If the content is not inappropriate, i.e., no match is found with any of the predetermined words or phrases, then the URL is added to the approved list on the database 120 at step 1530. After the URL has been added to the block list or to the approved list, the user is notified that the URL has been checked and is informed of the URL's status at step 1535. At step 1540, a determination is made whether there are any web pages linked to the web page associated with the checked URL. If there are associated web pages, then processing continues at step 1510 where the linked web page is downloaded and checked as described supra. If there are no associated web pages, then processing continues at step 1505 where the queue is checked to determine whether there are any more URLs to be checked.

When a requested URL returns Internet content to computer system 100, the BHO engages in a scan of the content as depicted in Figure 11. At step 1105, the BHO scans all of the content of the web page associated with the requested URL, including metatags and other hidden text. At step 1110, the BHO compares the scanned content from the web page to a list of predetermined words and phrases. If no matches are found between one of the predetermined words or phrases and the scanned content from the web page, then BHO content scanning ends at step 1130. If a match is found between one of the predetermined words or phrases and the scanned content from the web page, then the content of the web page is determined to be inappropriate at step 1110. A determination whether compliance with the Child On Line Privacy Protection Act of 1998 (COPPA), as implemented by 16 C.F.R. Part 312, exists is made at step 1115, and if not, the child is redirected to an access denied page 200 communicating with an access control server 115 at step 1125. Determining compliance with COPPA is, for example, a check to verify that a parent has granted permission for collecting the type of information that a web site desires to gather. If compliance with COPPA exists, then at step 1320 the BHO transmits the requested URL to an access control server 115 which adds the URL to a prohibited list on database 120 before proceeding to step 1325 where an access denied page is displayed.

PARENTAL QUERIES

Another aspect of the present invention is the ability of parents or guardians to view web sites that their children or wards have visited. By clicking on the "View a user's activity" icon (Figure 3), a parent or guardian may view a list of URLs that a particular child has visited. The parent or guardian is prompted to enter a child's username 1602, then a database query is performed, e.g., using SQL™, on the user table 1600, schematically shown in Figure 16, to retrieve zsuid 1604 (user identifier) associated with the child's username 1602. Once zsuid 1604 is retrieved, another database query is performed on the accessed URL table 1675. Because zsuid 1608 is linked to zsuid 1604, a list of URLs that the child has accessed, and when the child accessed each URL, is displayed for the parent or guardian.

DATA MINING QUERIES

Parents and guardians are not the only people interested in viewing what URLs children access on the Internet 105. Many companies are interested in such access information in order to improve products directed towards children and to learn how to direct advertising to children. The present invention allows the owner of database 120 to sell limited access to information contained in database 120. For example, a company that makes doll clothes would benefit from knowing what dolls girls are interested in, and what clothing styles girls interested in dolls like. A query performed on user table 1600 based upon gender and age could produce a list containing the zsuid 1604 of everyone in that category. A second query on accessed URL table 1675 utilizing every zsuid 1604 to link to a corresponding zsuid 1608 produces a list of URLs that everyone in the gender and age classification has visited, and when the visit occurred. The final list of URLs and when each URL was visited are valuable information that a doll clothes manufacturer can analyze for current trends, likes, dislikes, etc.

The present invention permits a consistent level of filtering of Internet content for a child, regardless of what copy of the client software a computer system the child is using is running. Parents are able to configure and monitor a child's Internet sessions from remote locations, and information is gathered that can be sold for marketing and research purposes.

Those skilled in the art will recognize, or be able to ascertain using no more than routine experimentation, many equivalents to the specific embodiments of the invention

BNSDOCID: <WO___0198934A2_I_>

specifically described herein. Such equivalents are intended to be encompassed in the scope of the following claims.

WHAT IS CLAIMED IS:

1. A method for granting access to internet content for a user, comprising the steps of:

transmitting a Uniform Resource Locator (URL) associated with internet content selected by the user and an identifier associated with the user from a first computer to an internet server;

determining at the internet server whether the user is to be granted access to the internet content by checking a database containing permitted URLs and prohibited URLs based upon access parameters associated with the identifier;

logging the URL in association with the identifier;

if the user is not to be granted access, then causing the first computer system to display an appropriate message;

if the user is to be granted access, then downloading the internet content associated with the URL onto the first computer system;

scanning the internet content by the first computer system to determine if one or more predetermined words or phrases are present in the internet content during said downloading; and

if said one or more predetermined words or phrases is present in the internet content, then terminating said downloading and logging the URL in the database as one of the prohibited URLs.

2. The method of claim 1, further comprising the steps of:

transmitting a second URL associated with internet content selected by the user and an identifier associated with the user to an internet server from a second computer system utilizing the second URL and the same identifier; and wherein

determining at the internet server whether the user is to be granted access to the internet content by checking a database containing permitted URLs and prohibited URLs based upon said access parameters associated with the identifier, to achieve an identical result as if the first computer system had been utilized to transmit the second URL;

logging the second URL in association with the identifier, to achieve an identical result as if the first computer system had been utilized to transmit the second URL;

if the user is not to be granted access, then causing the computer system to display an appropriate message, to achieve an identical result as if the first computer system had been utilized to transmit the second URL;

if the user is to be granted access, then downloading the internet content associated with the URL onto the computer system, to achieve an identical result as if the first computer system had been utilized to transmit the second URL;

scanning the internet content by the second computer system to determine if one or more predetermined words or phrases are present in the internet content during said downloading, to achieve an identical result as if the first computer system had been utilized; and

if said one or more predetermined words or phrases is present in the internet content, then terminating said downloading and logging the second URL in the database as one of the prohibited URLs.

3. The method of claim 1, further comprising the step of:

downloading an access profile for the user from the internet server onto the first computer; wherein the step of scanning comprises

determining if one or more predetermined words or phrases are present in the internet content during said downloading based upon the user's profile.

4. The method of claim 2, further comprising the step of:

downloading an access profile for the user from the internet server onto the second computer; wherein the step of scanning comprises

determining if one or more predetermined words or phrases are present in the internet content during said downloading based upon the user's profile.

5. The method of claim 1, wherein:

logging the URL in association with the identifier is performed on the first computer system; and further comprising the step of:

displaying on the first computer system a list of URLs that the user has accessed based upon the URL list logged on the first computer system.

6. The method of claim 1, wherein:

logging the URL in association with the identifier is performed on the internet server; and further comprising the step of:

displaying on the first computer system a list of URLs that the user has accessed based upon the URL list logged on the internet server.

7. The method of claim 6, wherein the step of displaying the list of URLs logged on the internet server comprises:

receiving a username at the first computer system;

transmitting the username to the internet server;

performing a database query on the database to identify URLs accessed using the username;

transmitting the results of the database query to the first computer system; and

displaying a list of URLs accessed using the username on the first computer system.

8. The method of claim 1, further comprising the step of:

displaying a list of URLs; wherein displaying the list of URLs comprises:

receiving a gender identifier and age range at the internet server;

performing a database query on the database to identify URLs accessed by users having the gender identifier and within the age range;

transmitting the results of the database query to the first computer system; and

displaying a list of URLs accessed by users having the gender identifier and within the age range on the first computer system.

9. The method of claim 1, wherein:

the first computer system runs a copy of software for granting access to internet content;

the internet server runs a copy of complementary software for granting access to internet content; and

the step of determining at the internet server whether the user is to be granted access to the internet content provides the same determination for the same user regardless of the particular copy of software for granting access to internet content run on the first computer system.

10. A method for granting access to internet content to a user, comprising the steps of:

transmitting a Uniform Resource Locator (URL) associated with internet content selected by the user and an identifier associated with the user from a first computer system;

receiving information at the first computer system regarding whether access is granted or denied;

logging the URL in association with the identifier;

if the user is not to be granted access, then displaying an appropriate message;

if the user is to be granted access, then downloading the internet content associated with the URL;

scanning the internet content to determine if one or more predetermined words or phrases are present in the internet content during said downloading; and

if said one or more predetermined words or phrases is present in the internet content, then terminating said downloading and transmitting the URL.

11. The method of claim 10, wherein:

logging the URL in association with the identifier is performed on the first computer system; and further comprising the step of:

displaying on the first computer system a list of URLs that the user has accessed based upon the URL list logged on the first computer system.

12. The method of claim 11, wherein displaying a list of URLs further comprises:

receiving a username at the first computer system;

transmitting the username;

receiving a list of URLs accessed by the username in response to transmitting the username; and

displaying on the first computer system a list of URLs that the user has accessed based upon the received URL list.

13. The method of claim 10, further comprising the step of:

displaying a list of accessed URLs; wherein displaying the list of URLs comprises:

receiving a gender identifier and age range at the first computer system;

receiving a gender identifier and age range;

receiving results of a database query in response to transmitting a gender identifier and age range; and

displaying a list of URLs accessed by users having the gender identifier and within the age range on the first computer system

14. A computer-readable medium bearing instructions for granting access to internet content to a user, said instructions, when executed, are arranged to cause a computer system to perform the steps of:

transmitting a Uniform Resource Locator (URL) associated with internet content selected by the user and an identifier associated with the user from a first computer system;

receiving information at the first computer system regarding whether access is granted or denied;

logging the URL in association with the identifier;

if the user is not to be granted access, then displaying an appropriate message;

if the user is to be granted access, then downloading the internet content associated with the URL;

scanning the internet content to determine if one or more predetermined words or phrases are present in the internet content during said downloading; and

if said one or more predetermined words or phrases is present in the internet content, then terminating said downloading and transmitting the URL.

15. A method for granting access to internet content by an internet server to a user, comprising the steps of:

receiving a Uniform Resource Locator (URL) associated with internet content requested by the user and an identifier associated with the user;

determining whether the user is to be granted access to the internet content by checking a first database containing permitted URLs and prohibited URLs based upon access parameters associated with the identifier;

transmitting whether the user is granted or denied access to the URL;

receiving information about the scanned content associated with the URL; and

if one or more predetermined words or phrases is present in the internet content, then logging the URL in the first database as one of the prohibited URLs.

16. The method of claim 15, wherein:

logging the URL in association with the identifier is performed on the internet server; and further comprising the step of:

displaying on a first computer system a list of URLs that the user has accessed based upon the URL list logged on the internet server.

17. The method of claim 15, further comprising the step of:

displaying a list of URLs; wherein displaying the list of URLs comprises:

receiving a username at the internet server;

BNSDOCID: <WO___0198934A2_I_>

performing a database query on the first database to identify URLs accessed using the username;

transmitting the results of the database query to a first computer system; and

displaying on the first computer system a list of URLs that the user has accessed based upon the transmitted URL list.

18. The method of claim 15, further comprising the step of:

displaying a list of URLs; wherein displaying the list of URLs comprises:

receiving a gender identifier and age range at the internet server;

performing a database query on the first database to identify URLs accessed by users having the gender identifier and within the age range;

transmitting the results of the database query to a first computer system; and

displaying a list of URLs accessed by users having the gender identifier and within the age range on the first computer system

19. A computer-readable medium bearing instructions for granting access to internet content by an internet server to a user of a first computer system, said instructions, when executed, are arranged to cause the internet server to perform the steps of:

receiving a Uniform Resource Locator (URL) associated with internet content requested by the user and an identifier associated with the user;

determining whether the user is to be granted access to the internet content by checking a first database containing permitted URLs and prohibited URLs based upon access parameters associated with the identifier;

transmitting whether the user is granted or denied access to the URL;

receiving information about the scanned content associated with the URL; and

if one or more predetermined words or phrases is present in the internet content, then logging the URL in the first database as one of the prohibited URLs

20. A method for granting access to a user to internet content, comprising the steps of:

transmitting a Uniform Resource Locator (URL) associated with internet content selected by the user and an identifier associated with the user from a first computer system to an internet server;

downloading onto the first computer system an access control profile associated with the user's identifier;

BNSDOCID: <WO___0198934A2_I_>

determining at the internet server whether the user is to be granted access to the internet content based upon access parameters associated with the identifier;

if the user is not to be granted access, then causing the first computer system to display an appropriate message;

if the user is to be granted access, then downloading the internet content associated with the URL onto the first computer system;

scanning the internet content by the first computer system to determine if one or more predetermined words or phrases are present in the internet content during said downloading based upon the downloaded access control profile; and

if said one or more predetermined words or phrases is present in the internet content, then terminating said downloading.

21. The method of claim 20, further comprising the step of:

if said one or more predetermined words or phrases is present in the internet content, then updating the access parameters associated with the identifier residing on the second system with information pertaining to the URL for which access was denied.

22. The method of claim 21, further comprising the step of:

logging the URL and identifier if access to the URL is granted and no predetermined words or phrases are present in the internet content.

23. The method of claim 22, further comprising the step of:

displaying on the first computer system the log of URLs and the associated identifier.

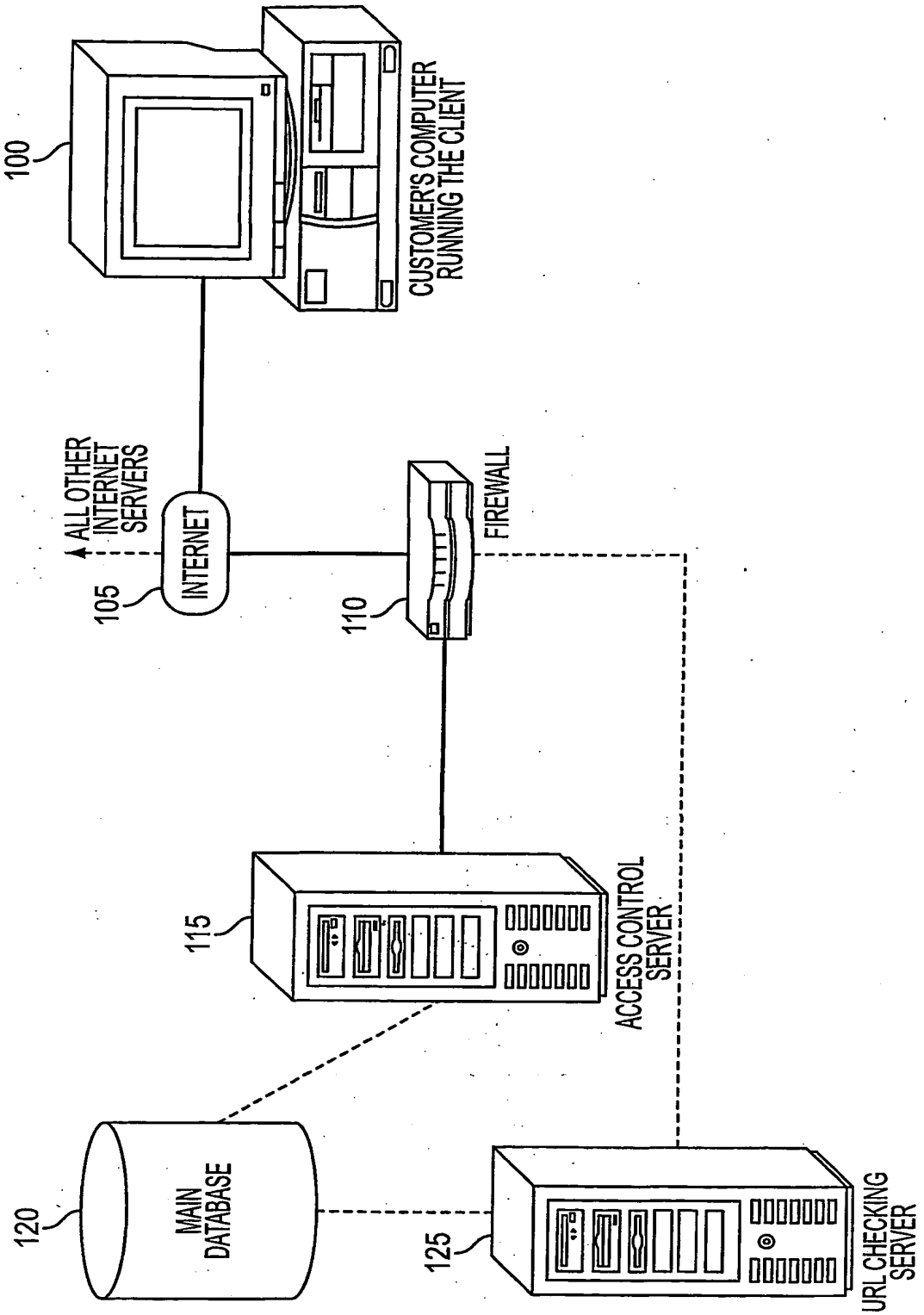


FIG. 1

BNSDOCID: <WO___0198934A2_I_>

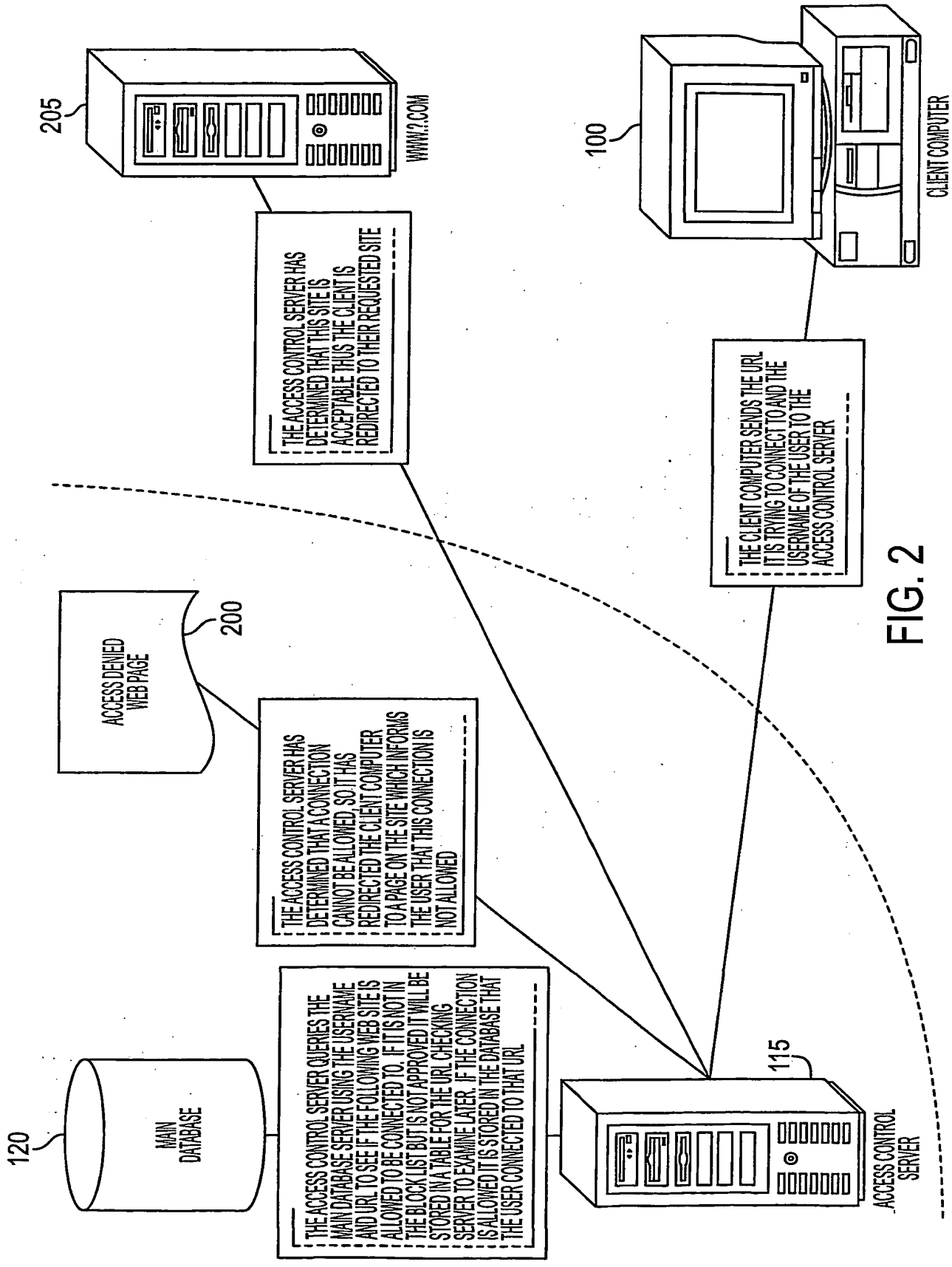


FIG. 2

BNSDOCID: <WO___0198934A2_I_>

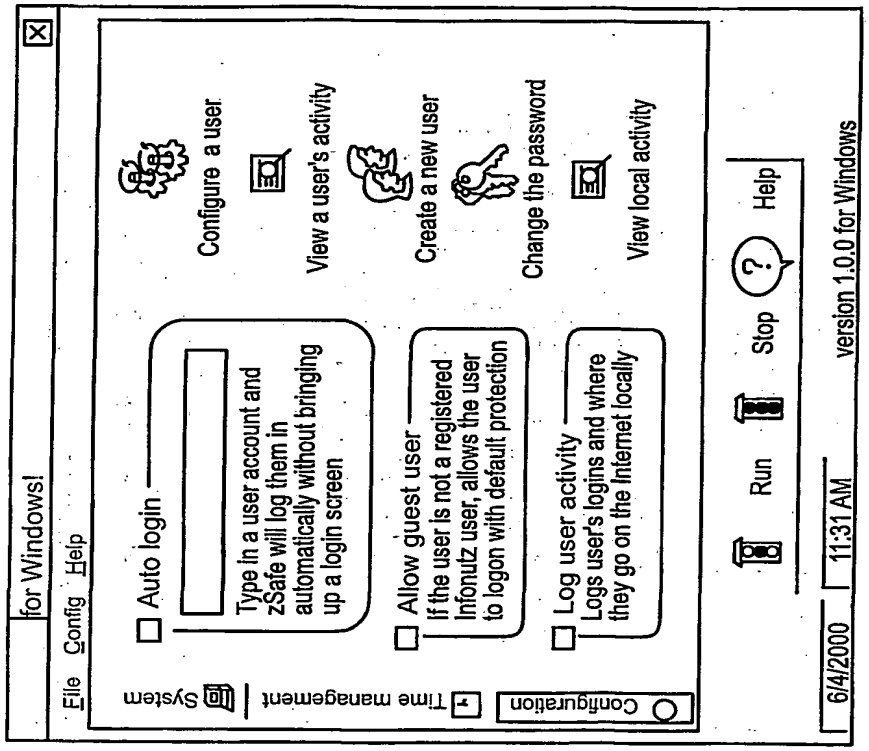


FIG. 3

BNSDOCID: <WO___0198934A2_I_>

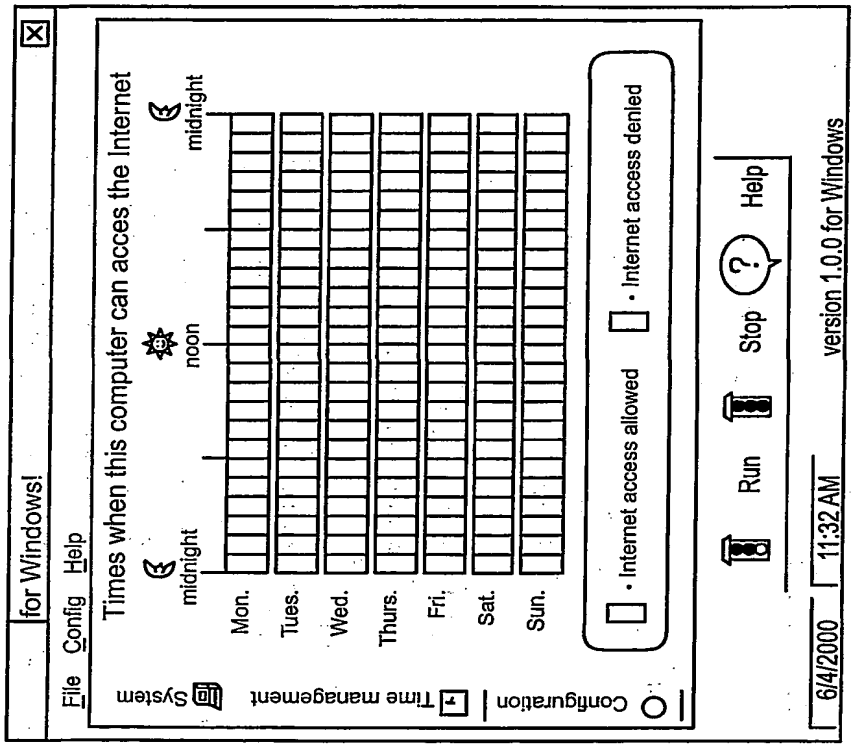


FIG. 4

BNSDOCID: <WO___0198934A2_I_>

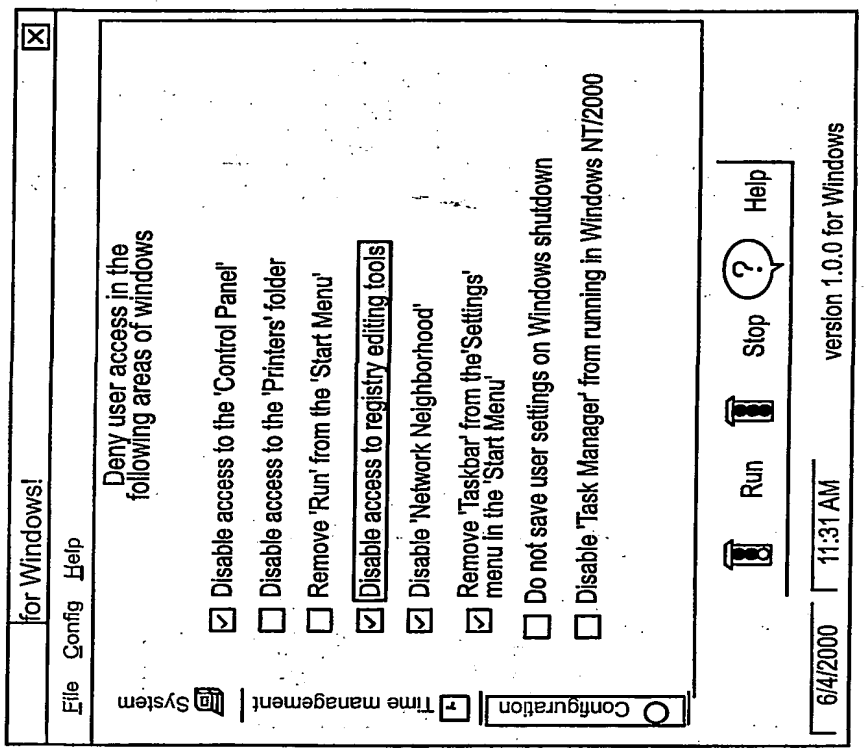


FIG. 5

BNSDOCID: <WO___0198934A2_I_>

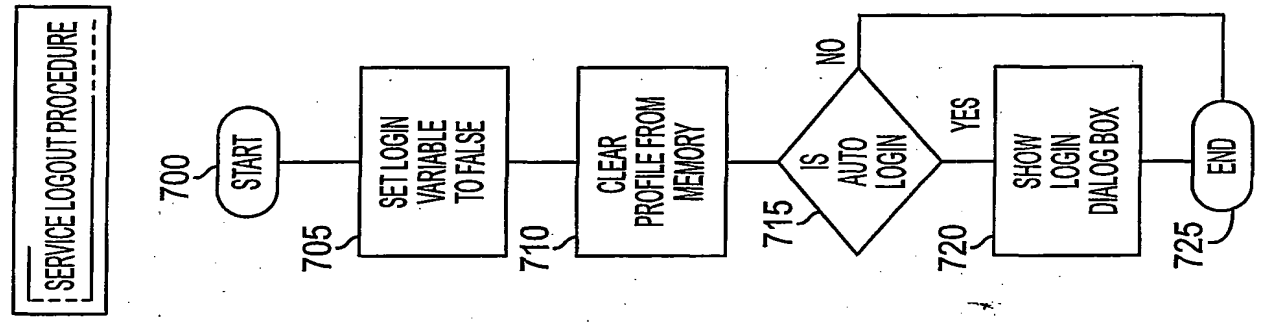


FIG. 7

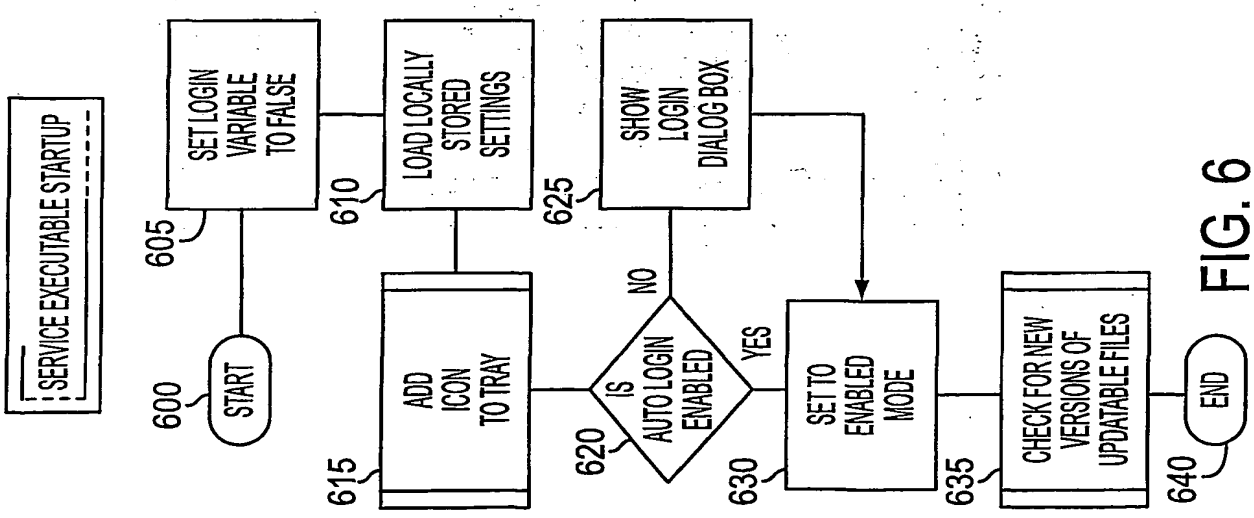


FIG. 6

BNSDOCID: <WO___0198934A2_I_>

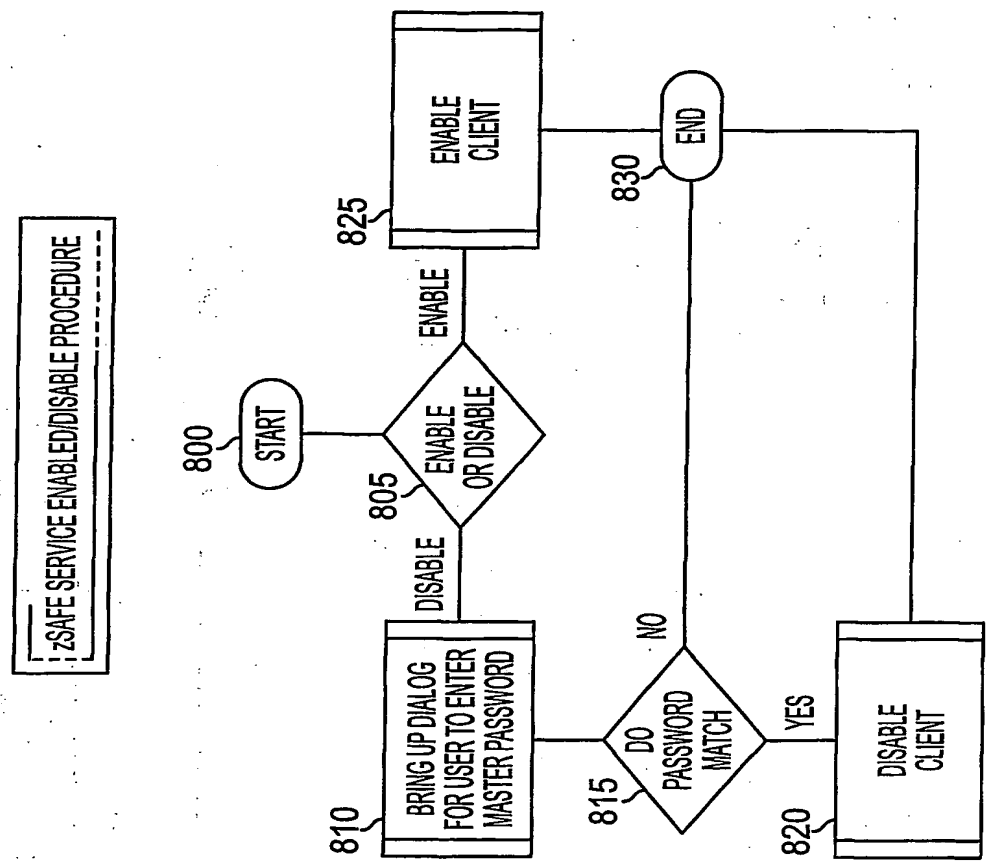


FIG. 8

BNSDOCID: <WO___0198934A2_I_>

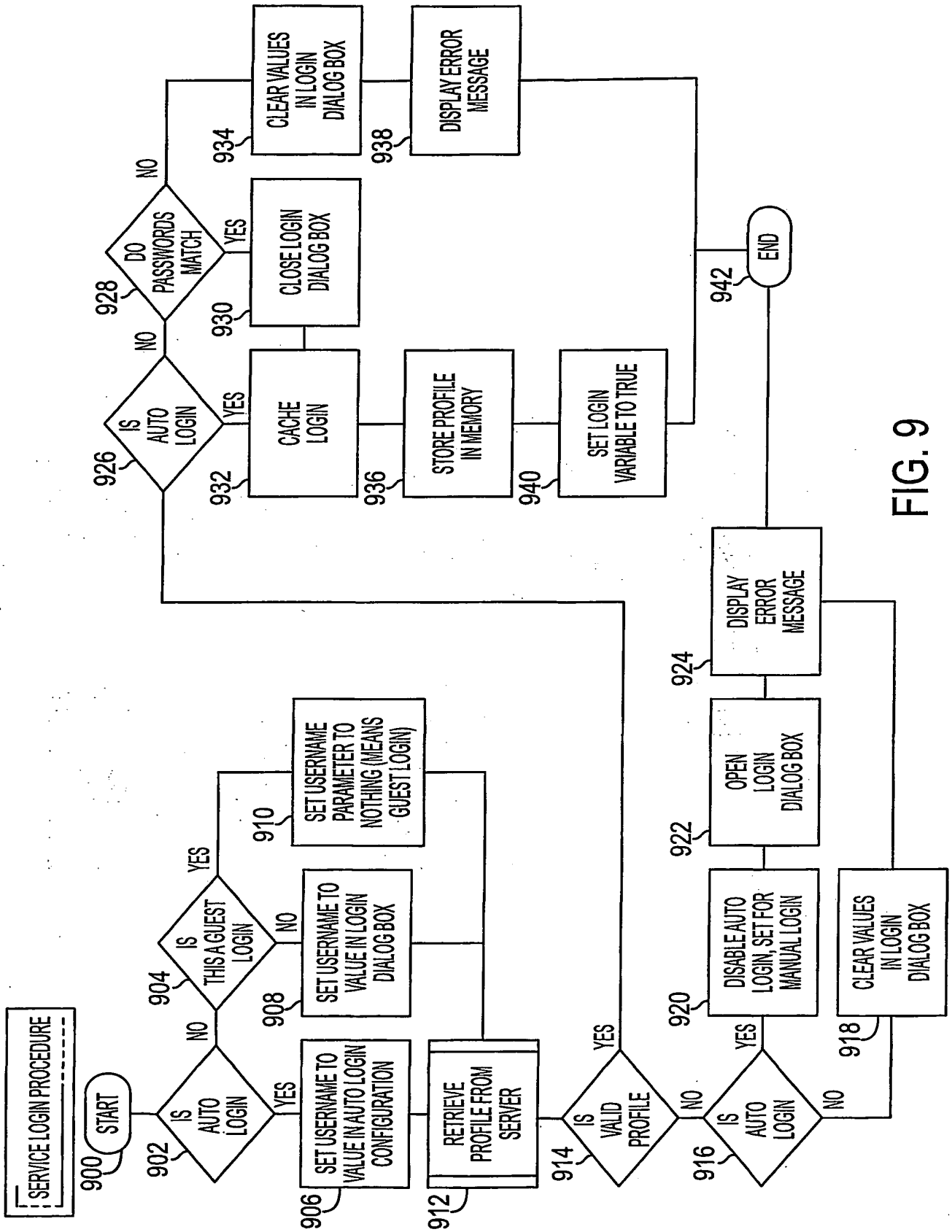


FIG. 9

BNSDOCID: <WO___0198934A2_I_>

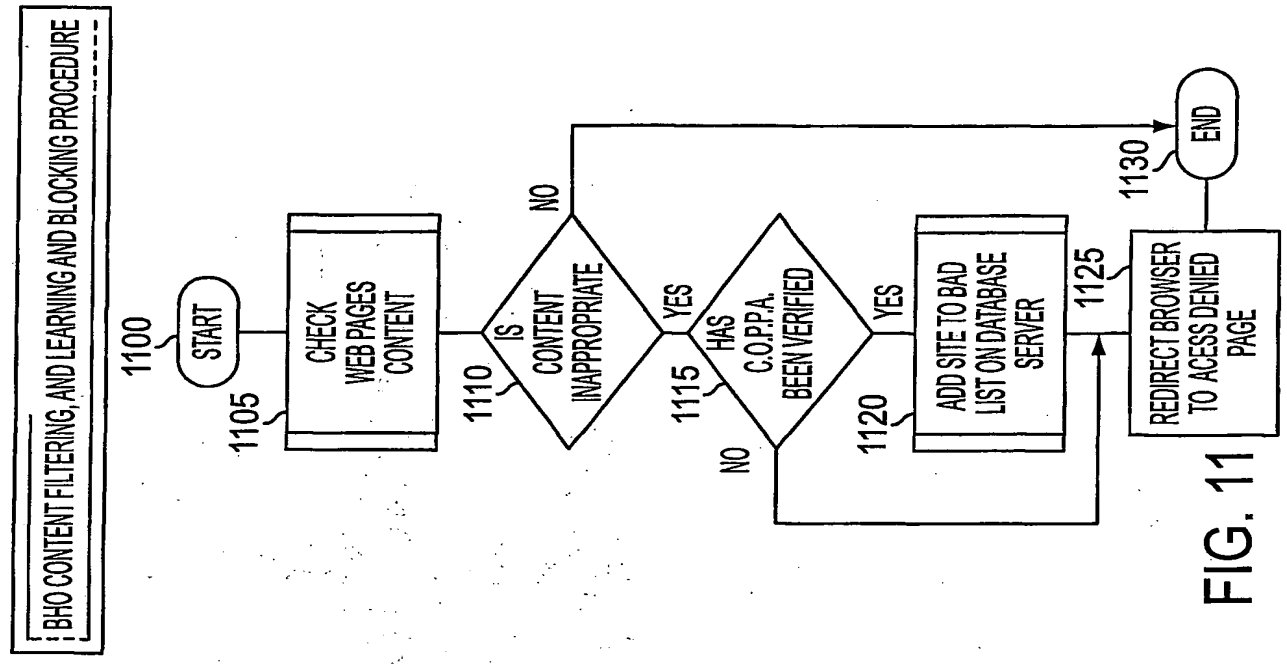


FIG. 11

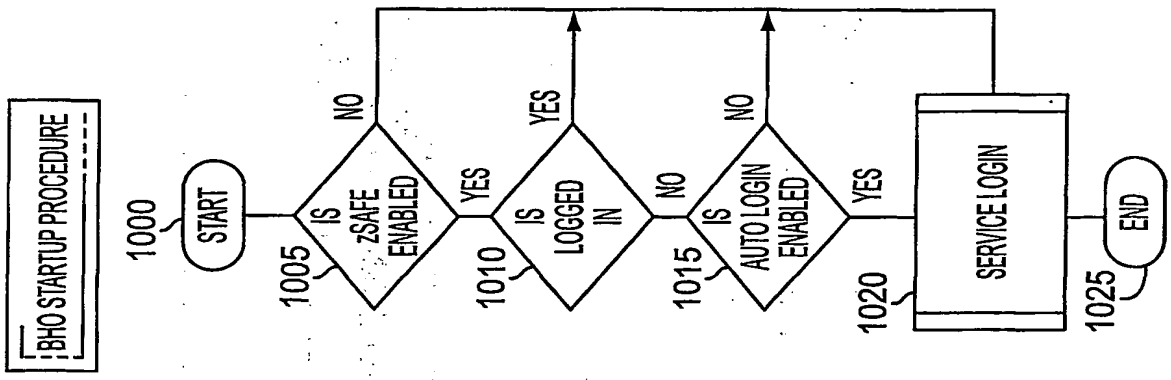


FIG. 10

BNSDOCID: <WO___0198934A2_I_>

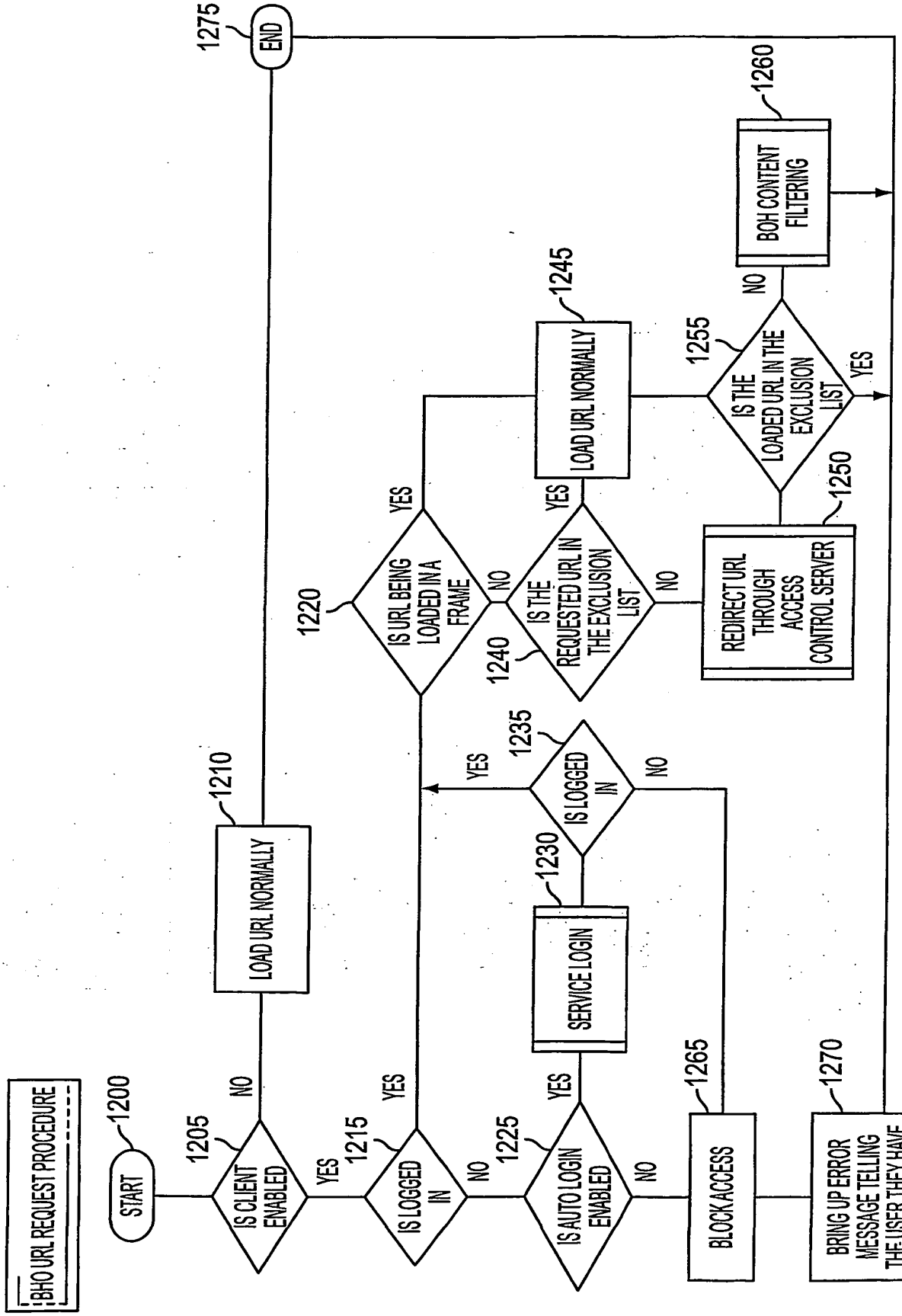


FIG. 12

BNSDOCID: <WO___0198934A2_I_>

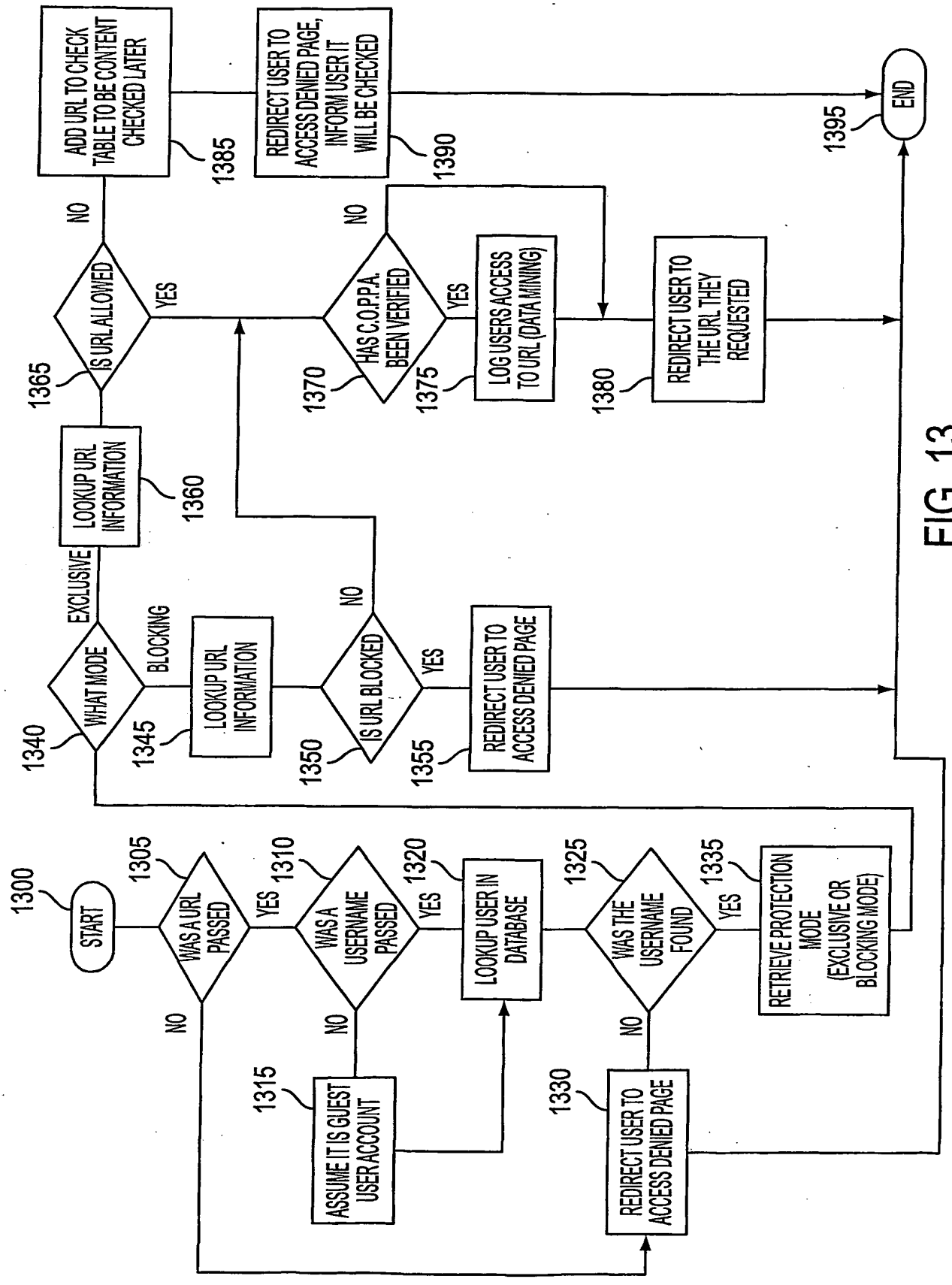


FIG. 13

BNSDOCID: <WO___0198934A2_I_>

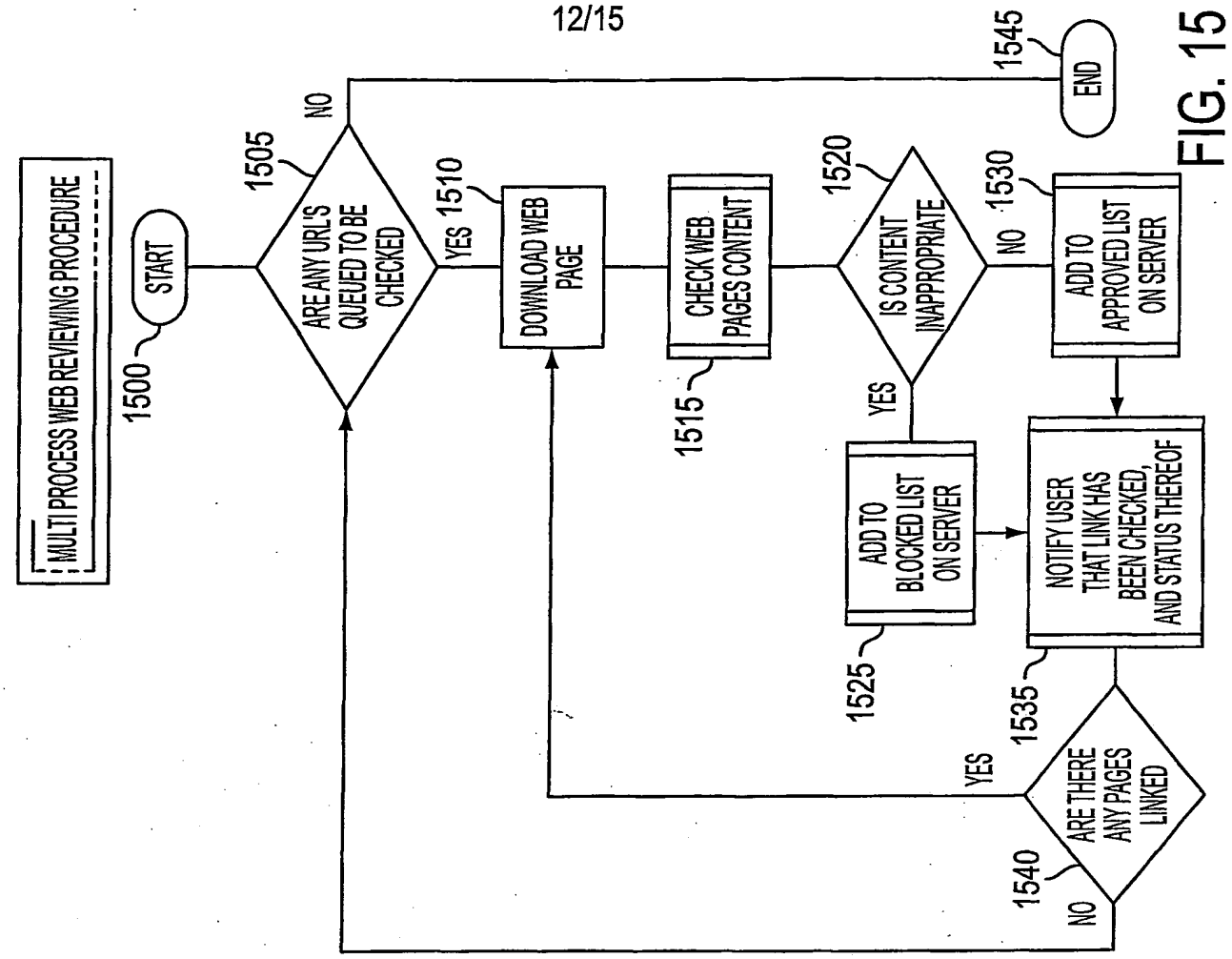


FIG. 15

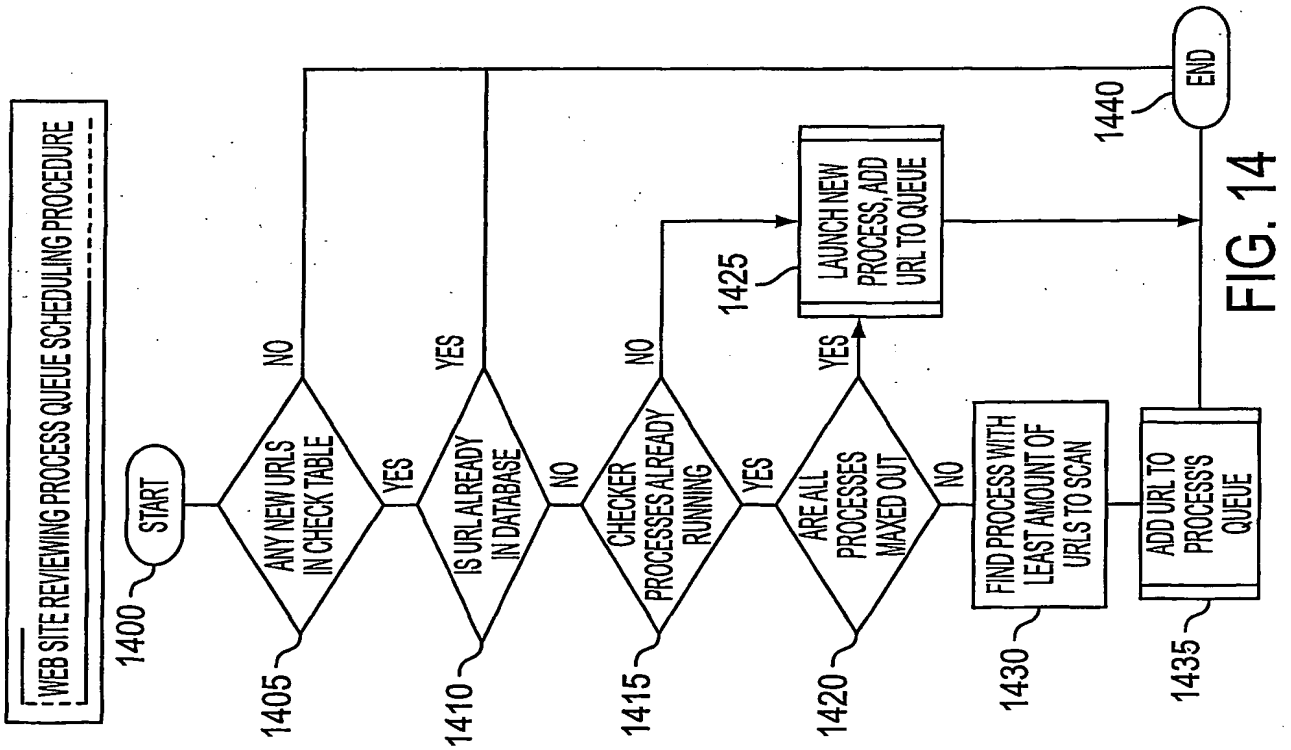


FIG. 14

BNSDOCID: <WO___0198934A2_I_>

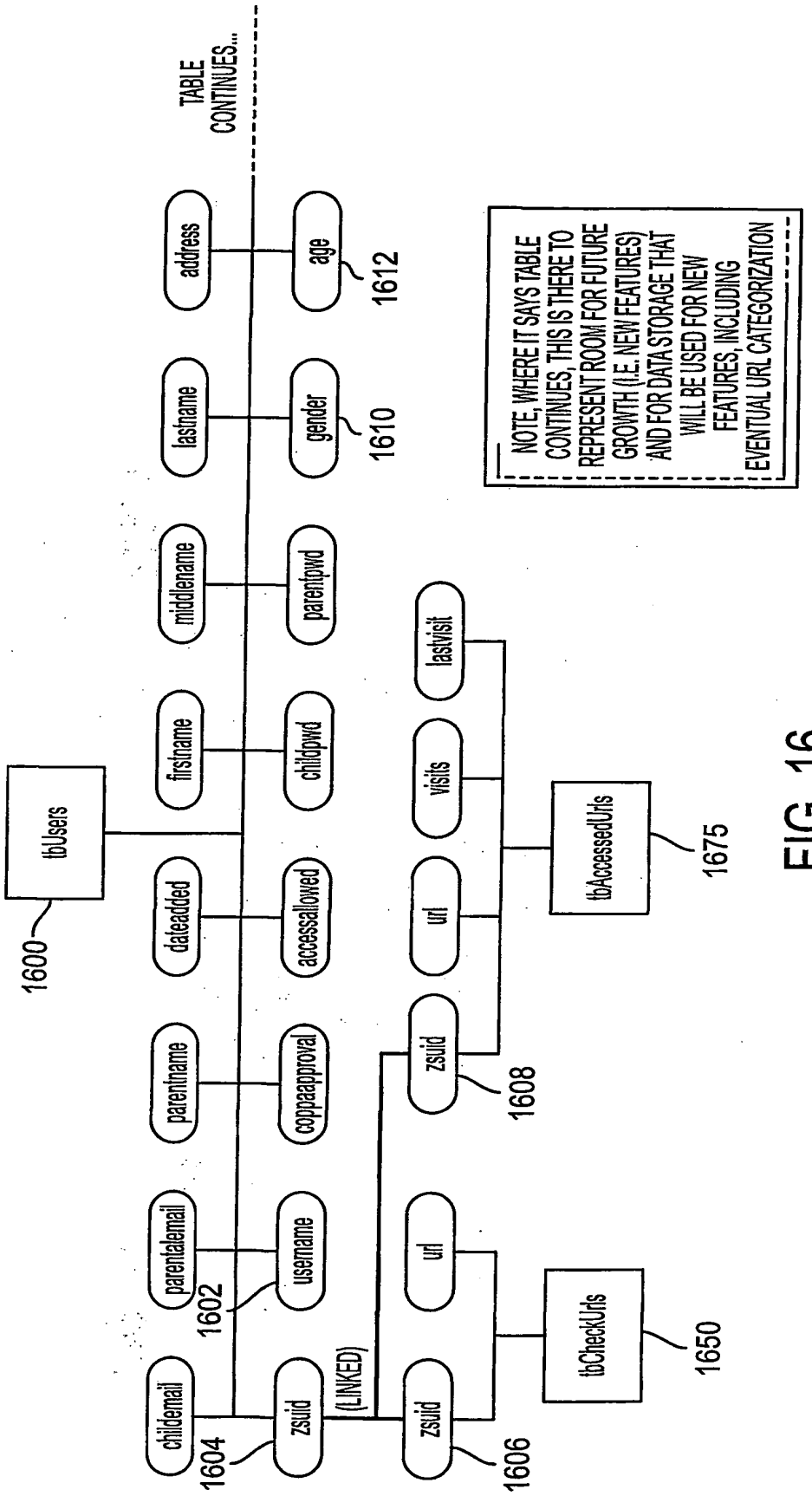


FIG. 16

BNSDOCID: <WO___0198934A2_I_>

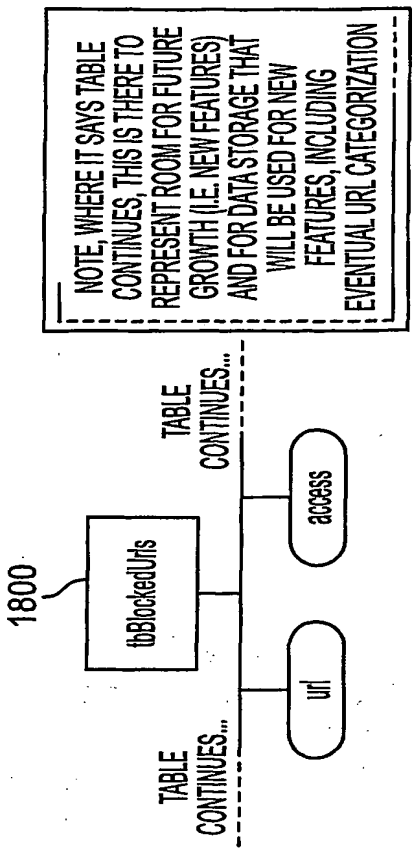


FIG. 18

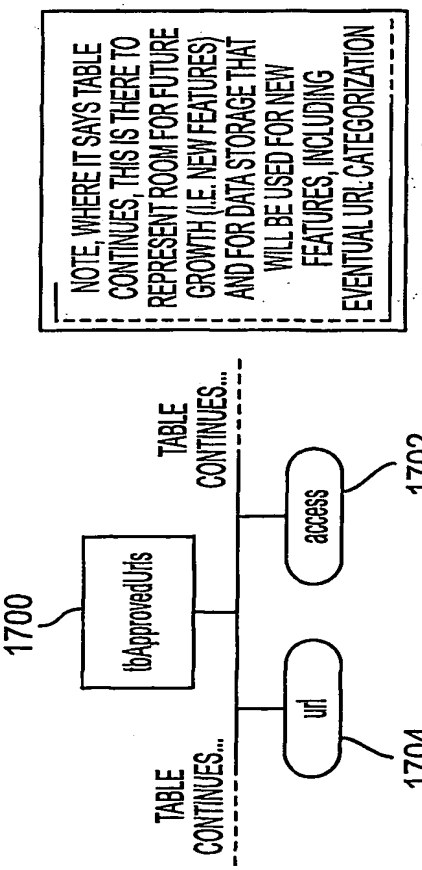


FIG. 17

BNSDOCID: <WO___0198934A2_I_>

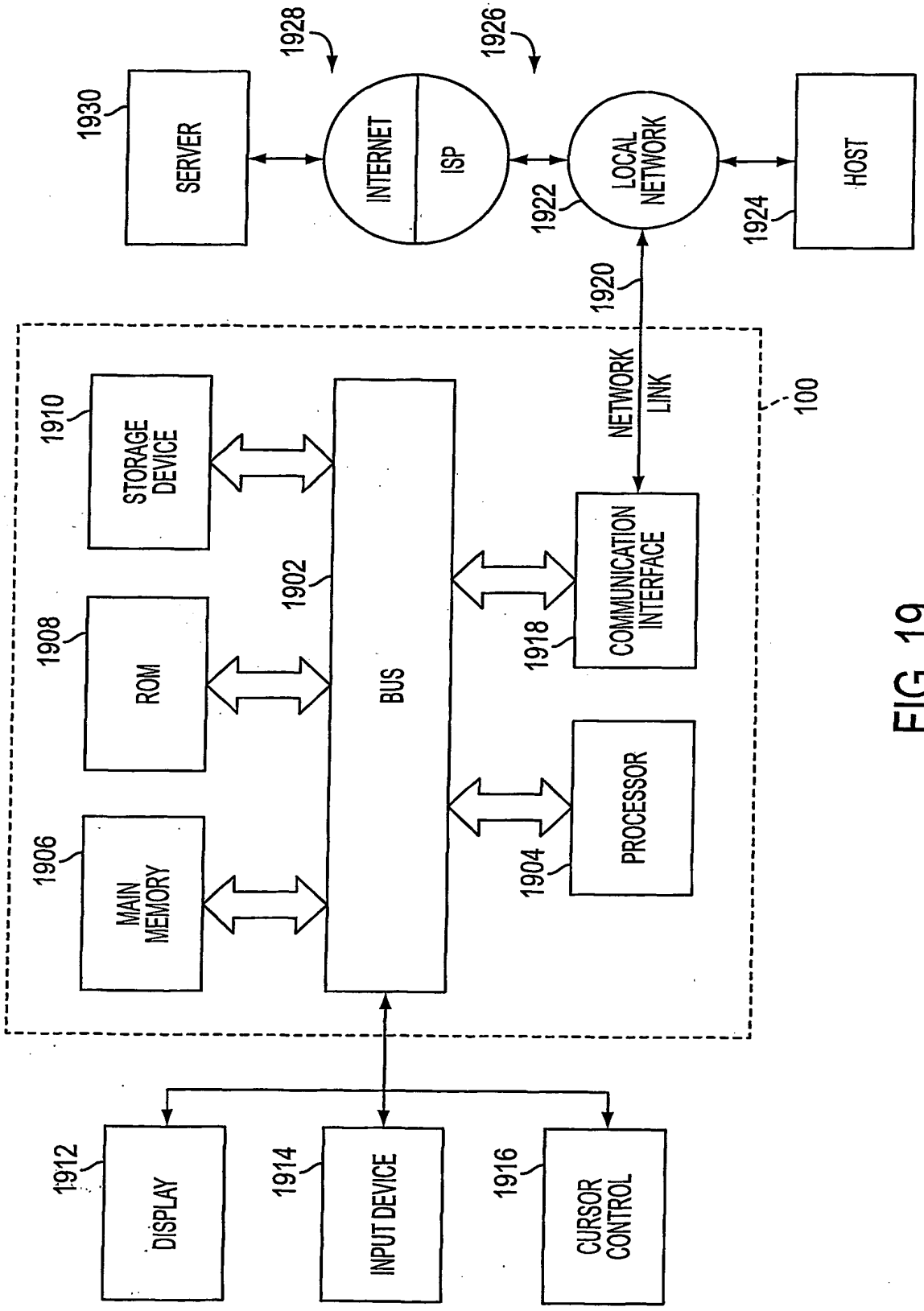


FIG. 19

BNSDOCID: <WO___0198934A2_I_>

THIS PAGE BLANK (USPTO)